(19)美国。

美国 20180373984A1。

(12)专利申请公开(10)。编号：美国 2018 年/0373984 Al。

Katz et al.。

(43)酒吧。日期：　2018 年 12 月 27 日。

ONE OR ET 翻译

(54)具有分离的安全功能和公共功能的体系结构、系统和方法。

(71) 申请人：里程碑式的娱乐。
有限责任公司，加利福尼亚州贝弗利山庄(美国)。

(72) 发明者：兰德尔・M・卡茨，贝弗利山。
加州(美国)；罗伯特・特里克(Robert TERCEK)，好莱坞，加利福尼亚州(美国)。

(21) APPL。编号：16/052,470。

(22) 提交：　2018 年 8 月 1 日。

相关的美国申请数据。

(63)延续 2018 年 2 月 1 日提交的第 15/886,432 号申请。

(注 60)临时申请第 62/454,423 号，于 2017 年 2 月 3 日提交。

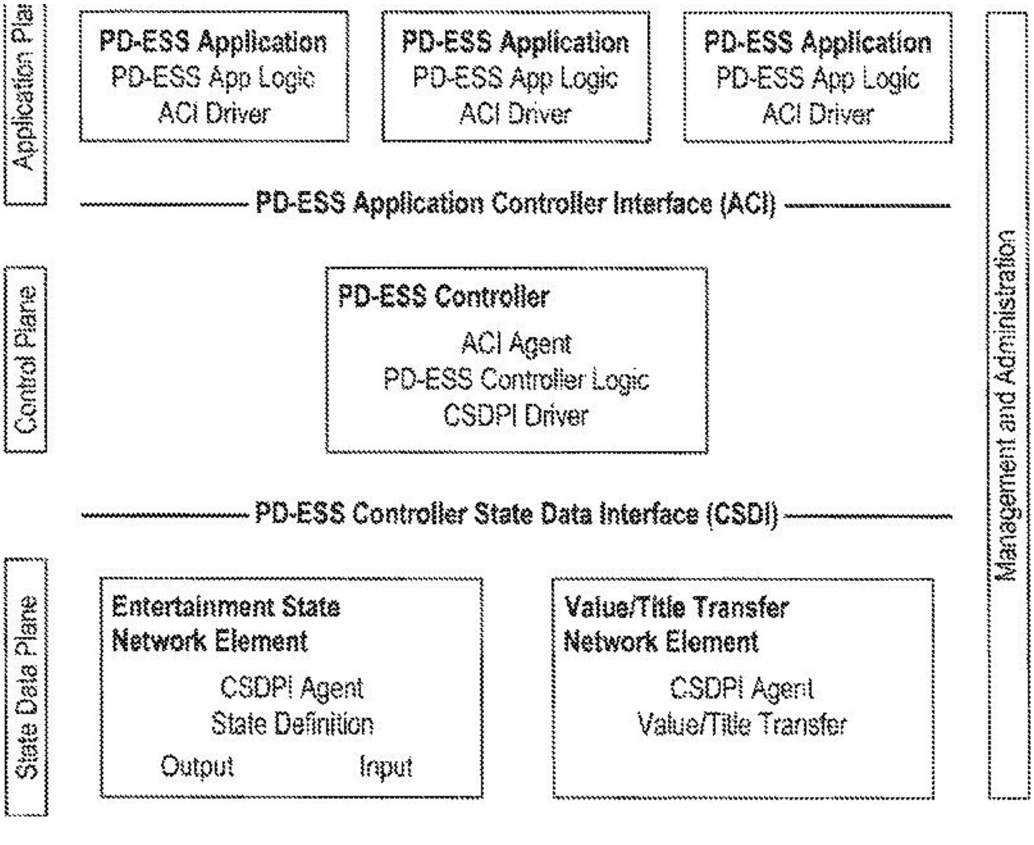
出版物分类。

(51)内部。克莱。
G06N 3/08(2006.01)。
G07F17/32(2006.01)。
G06K 9/00(2006.01)。
G06Q 20/06(2006.01)。

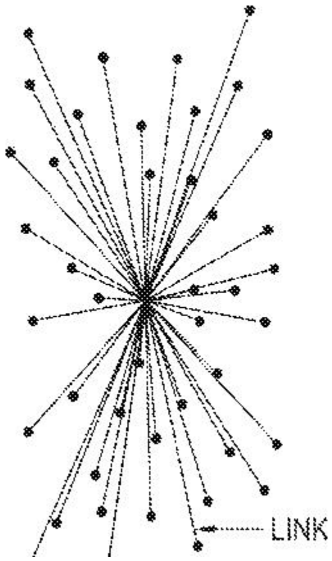
(52)美国。
CPCG06N 3/08(2013.01)；G07F *17/329*。
(2013.01)；G06Q20/065(2013.01)；G06K
9/00221(2013.01)。

(57)摘要。

向系统提供对娱乐状态系统的 FBR 控制，该娱乐状态系统具有由系统的一个或多个用户使用的分离的安全功能和公共功能 FBR。首先，公共接口门户从一个或多个用户接收关于娱乐状态系统的操作的指令。接口入口包括第一接口、处理器、耦合到处理器的图形用户接口(GUI)、与处理器和图形用户接口进行操作通信的控制单元、以及提供应用程序接口(API)的第二接口。其次，提供安全实体单元，该安全实体单元包括接收接口、适于从接口门户的应用程序接口(API)接收调用的接收接口、发送接口、适于提供对接口门户接口的响应的发送接口、游戏引擎和金融引擎。



定义的 Gsnimg 系统。

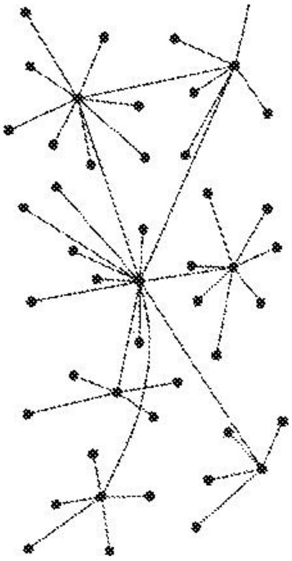


车站。

ONTRaUZED(A)PONOR 艺术集中系统。

H或7。

(前阿里)。

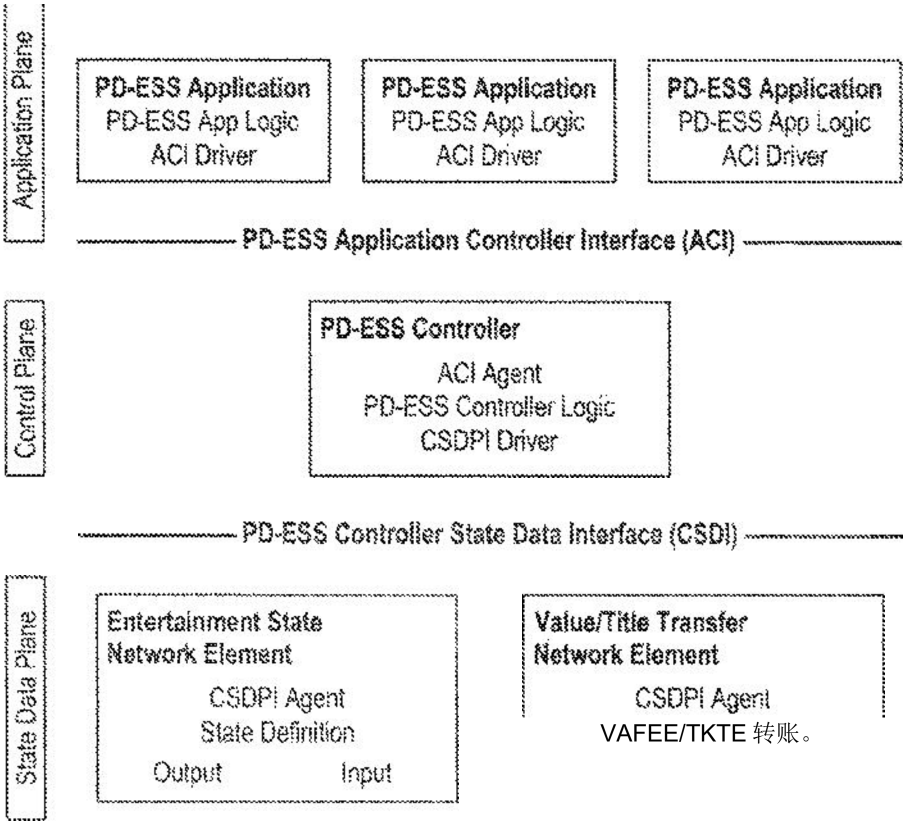


偏心^边。

糟糕的艺术体系。

*插图。*2

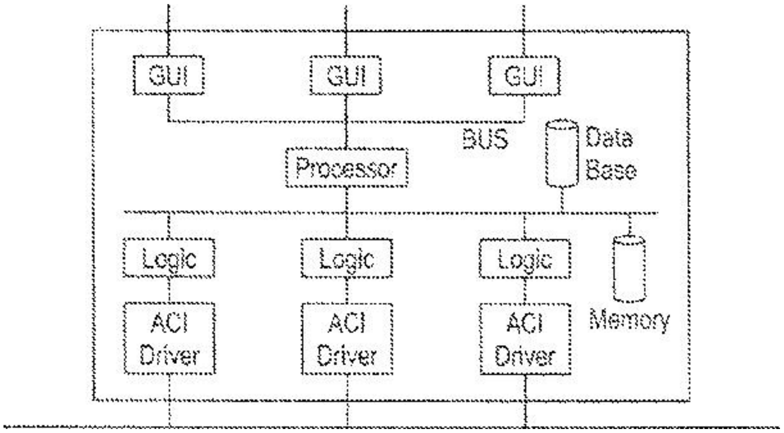
现有技术)。



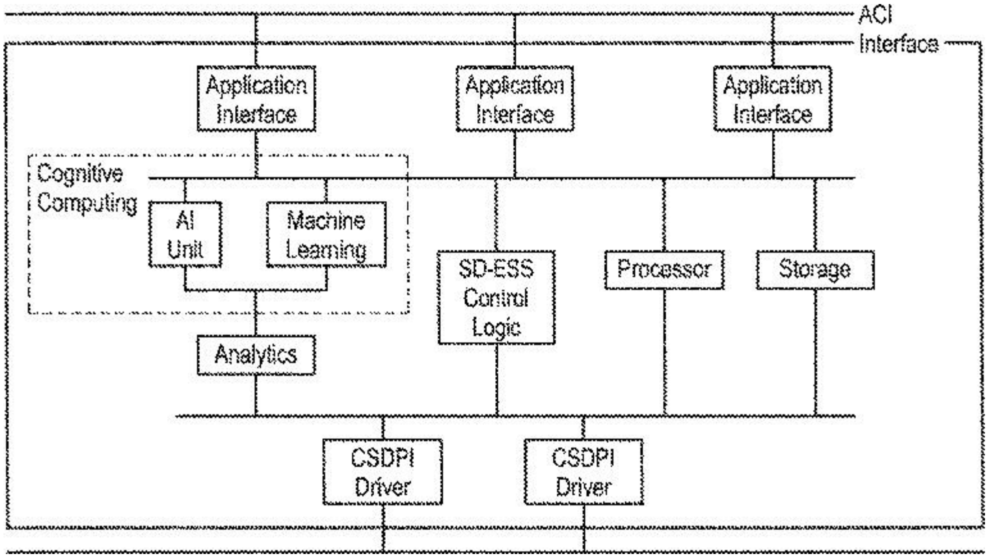
UA/1-g ‘g<I*SE®SJ ※%s。

Programmatically Defined Gaming System

插图。3



Applseatton Ptarss Lsyer 伸缩术。

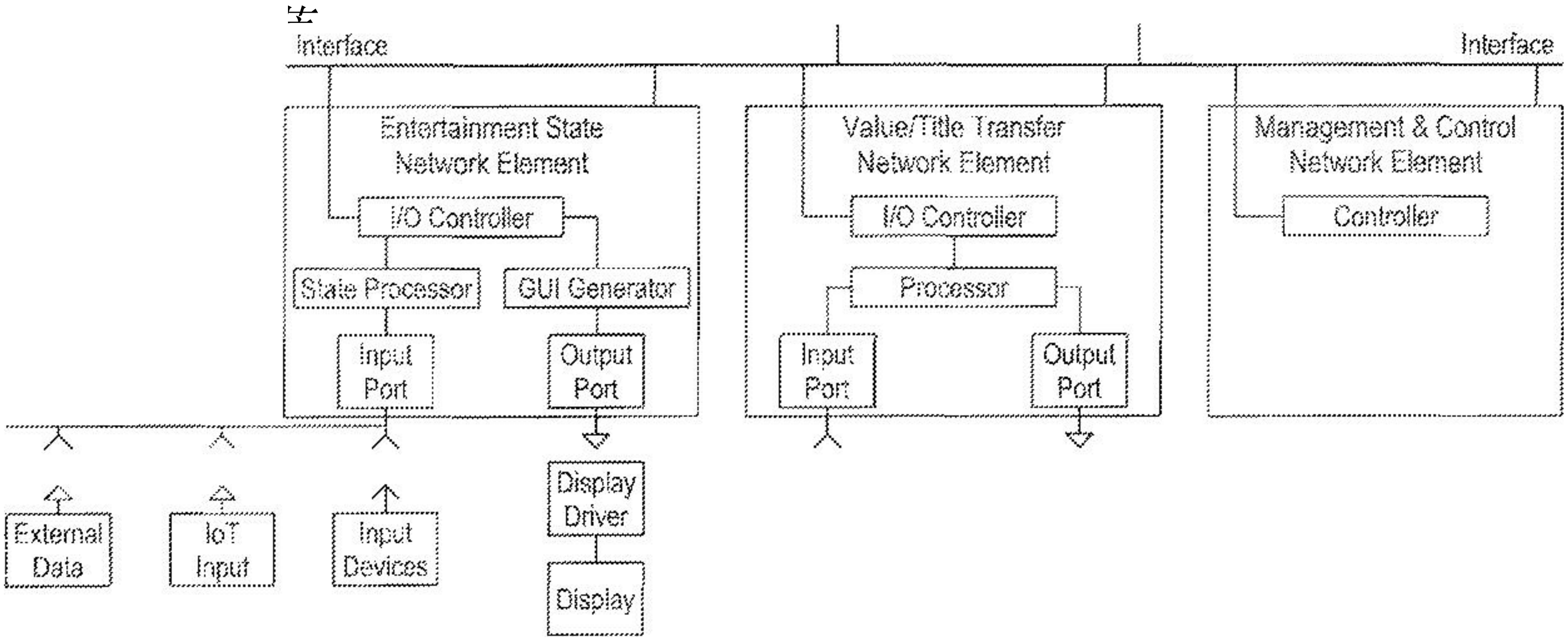


CSD^接
口。

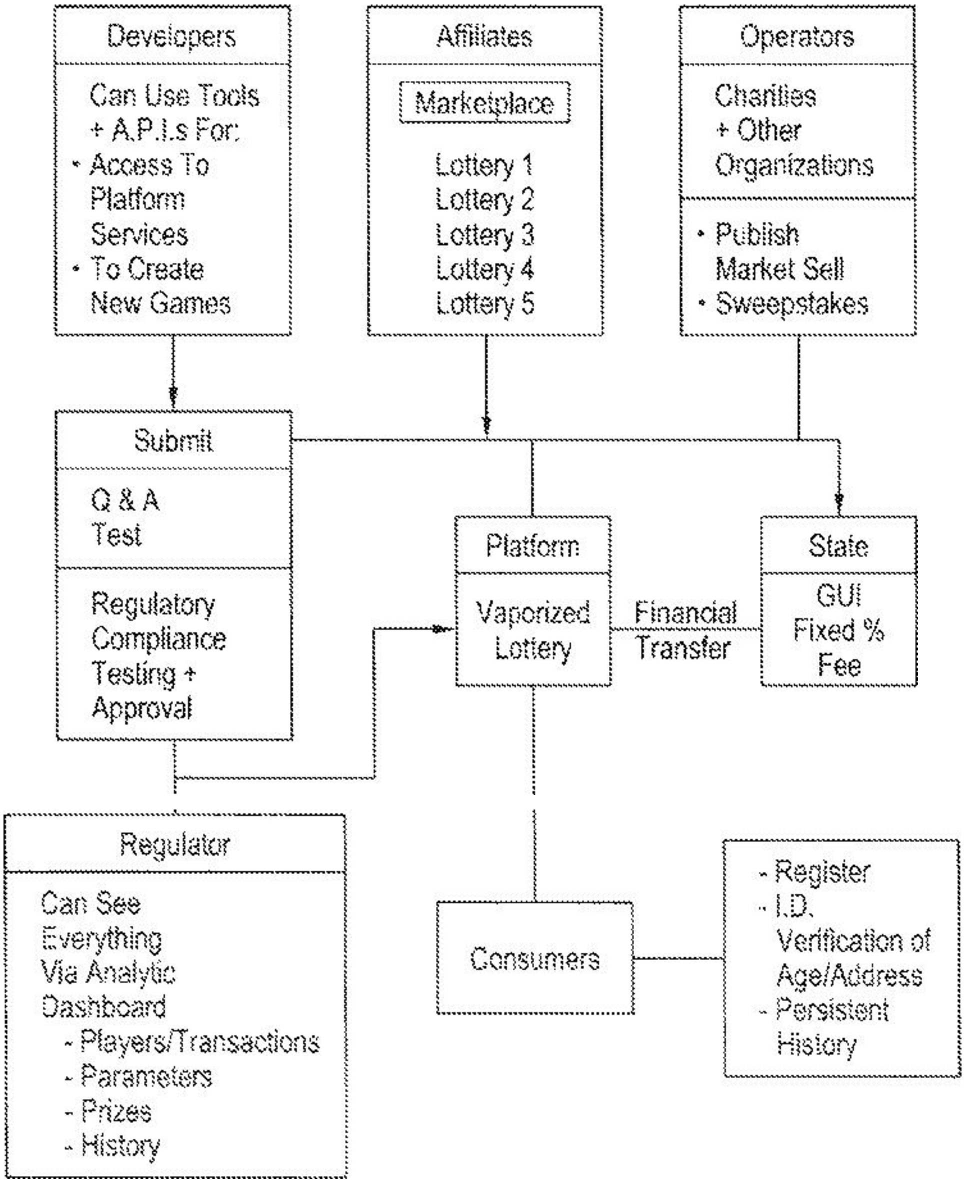
CSDI阶
梯。

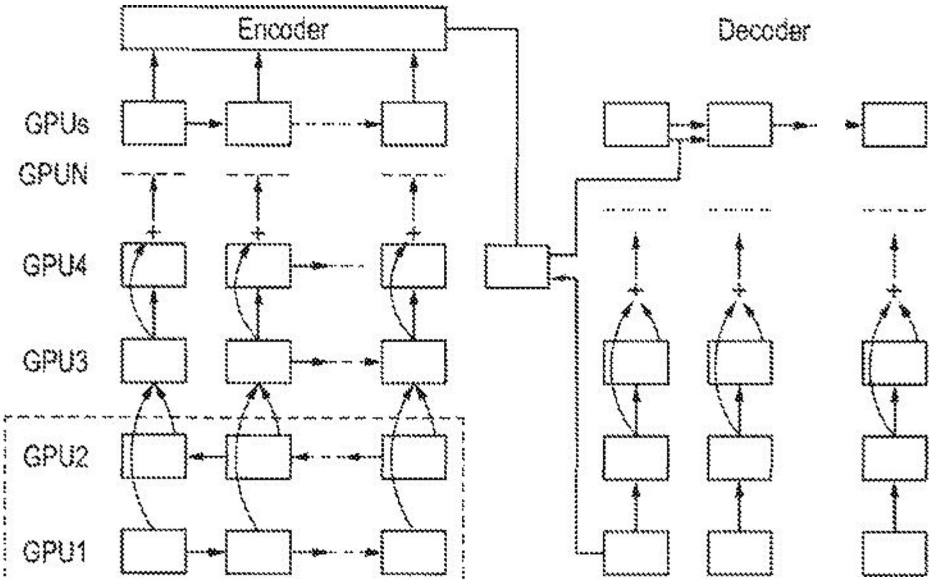
控制平面分层爆炸。

H板。



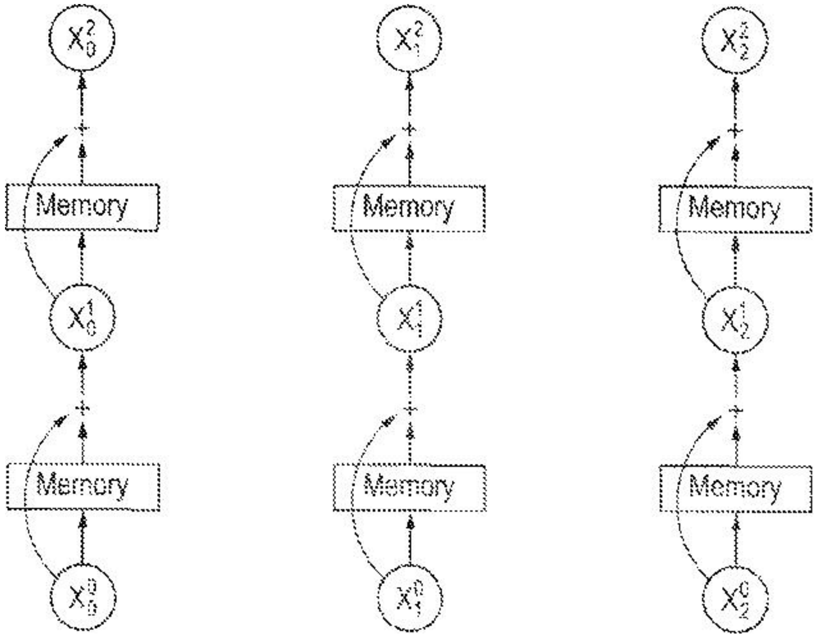
CKW Wen 段羔蕴将舞


Developers
Can Use Tools + A.P.I.s For:
• Access To Platform Services
• To Create New Games
Affiliates
Marketplace
Lottery 1
Lottery 2
Lottery 3
Lottery 4
Lottery 5
Operators
Charities + Other Organizations
• Publish Market Sell
• Sweepstakes
Submit
Q & A
Test
Regulatory Compliance Testing + Approval
Platform
Vaporized Lottery
Financial Transfer
State
GUI
Fixed %
Fee
Regulator
Can See Everything Via Analytic Dashboard
- Players/Transactions
- Parameters
- Prizes
- History
Consumers
- Register
- I.D. Verification of Age/Address
- Persistent History



Neural Network Model Architecture

FIG. 8



履㈱福芯嫩的值。

*插图。*0

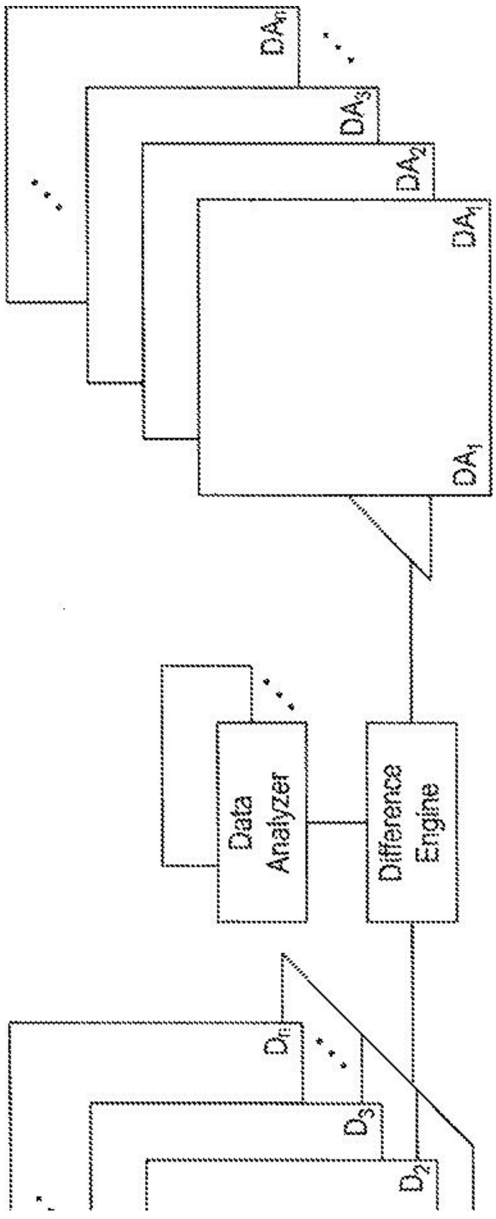


FIG. 10

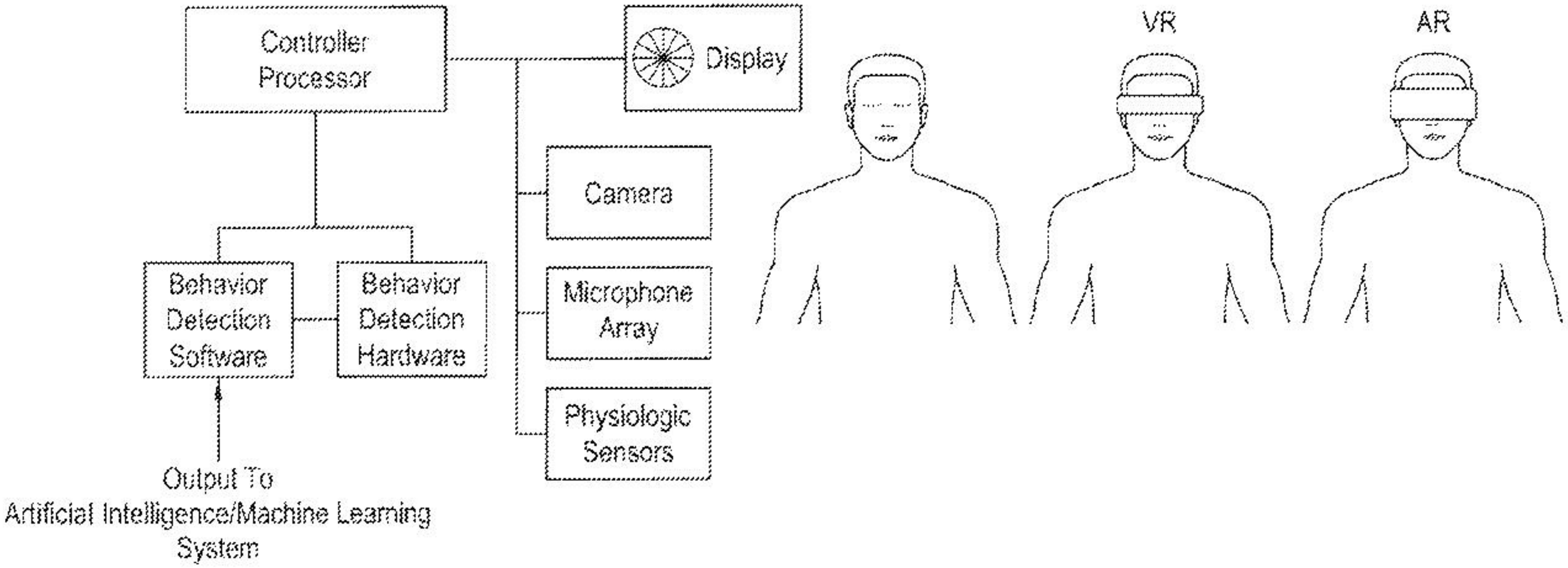
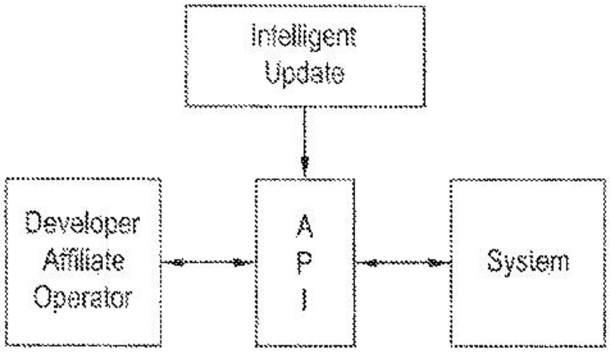
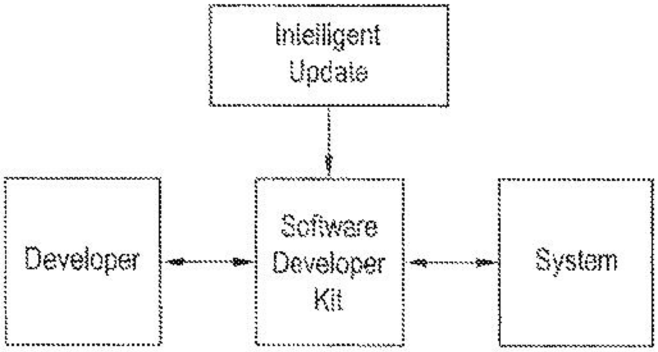

Controller
Processor
Display
Camera
Microphone
Array
Physiologic
Sensors
Behavior
Detection
Software
Behavior
Detection
Hardware
Output To
Artificial Intelligence/Machine Learning
System
VR
AR

FIG. 11



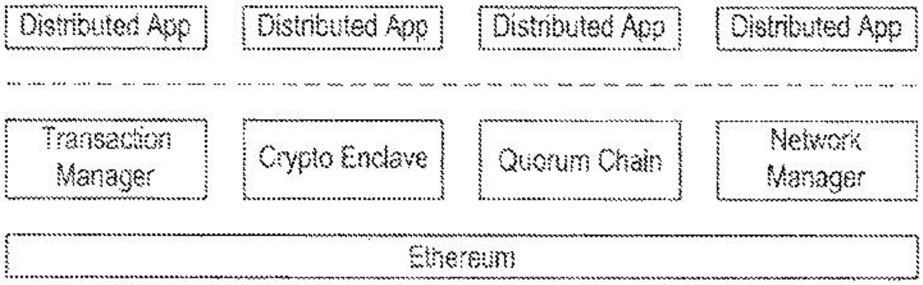
Dynamic Systems d-API

FIG. 12



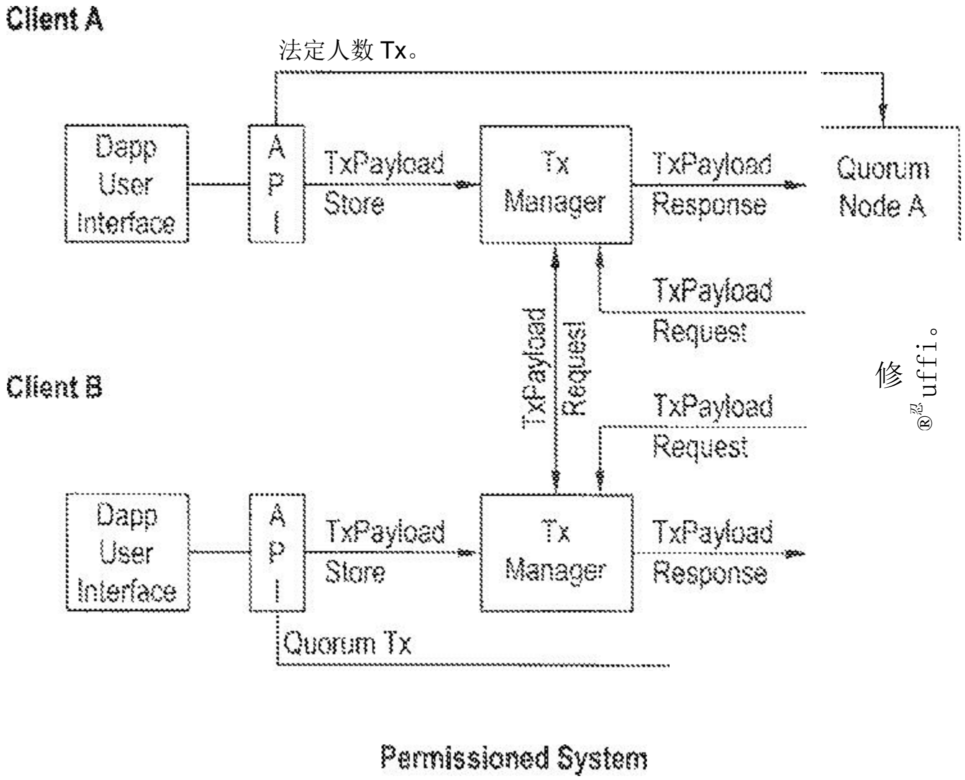
Dynamic Systems d-SDK

FIG. 13

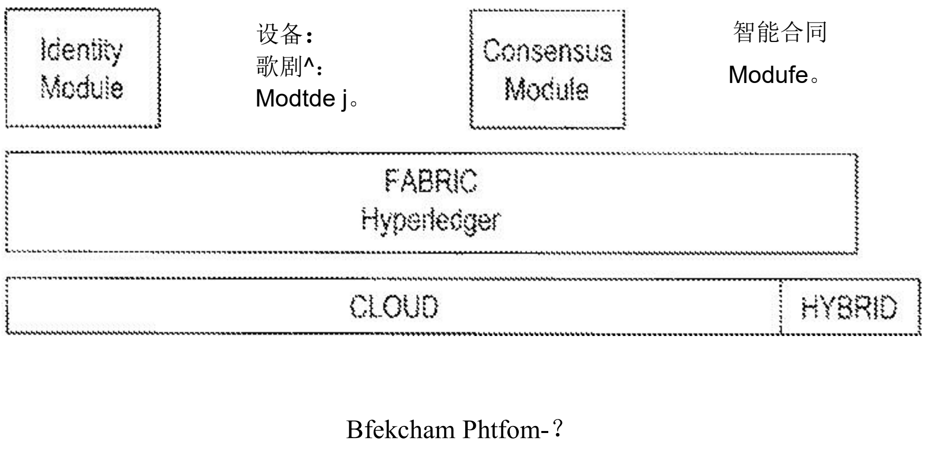


Architecture

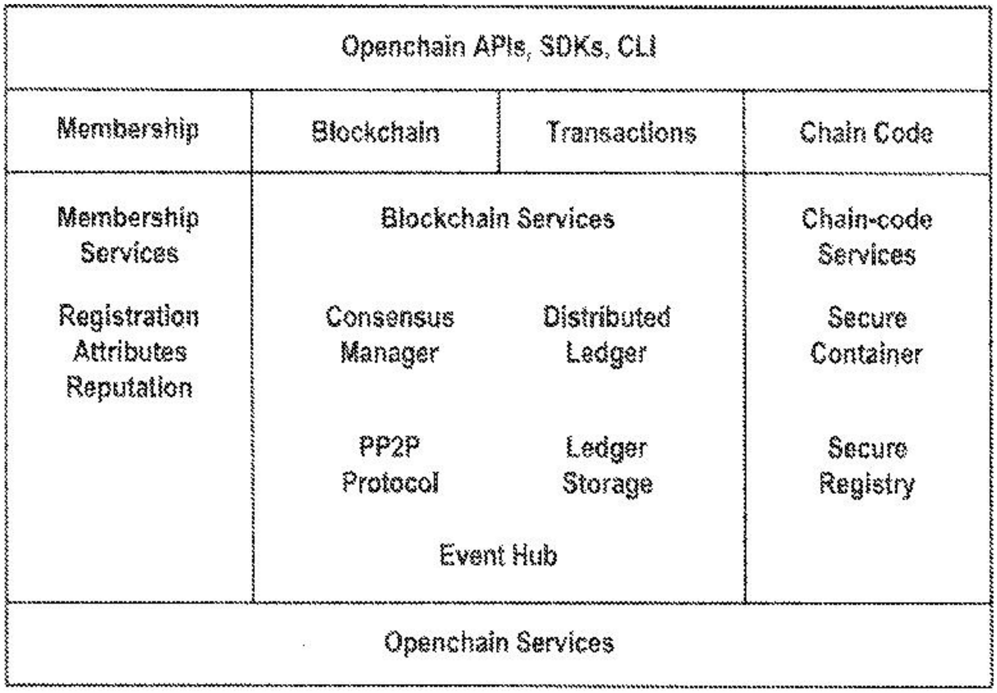
FIG. 14


Client A
法定人数 Tx。
Dapp User Interface
A P I
TxPayload Store
Tx Manager
TxPayload Response
Quorum Node A
TxPayload Request
TxPayload Request
Client B
修
®uffi。
TxPayload Request
Dapp User Interface
A P I
TxPayload Store
Tx Manager
TxPayload Response
Quorum Tx
Permissioned System

HIX JO。

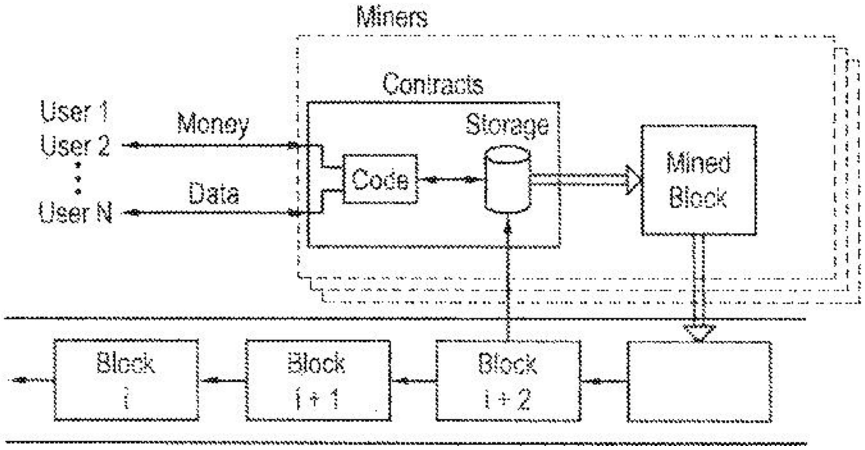

Identity Module
设备：
歌剧^：
Modtde j。
Consensus Module
智能合同
Modufe。
FABRIC Hyperledger
CLOUD
HYBRID
Bfekcham Phtfom-？

插图。16



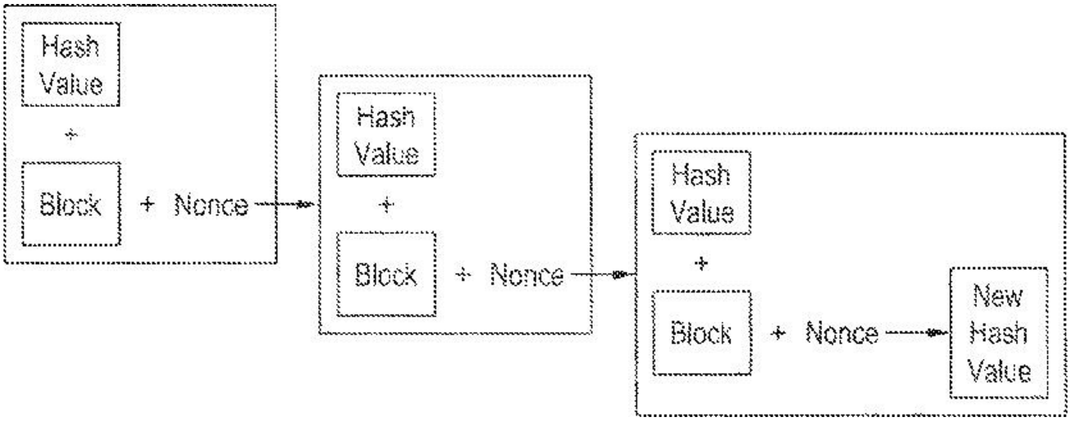
Platform

FIG. 17



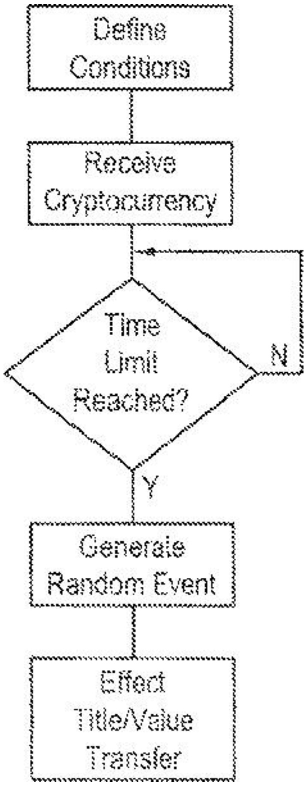
一个C++并行程序的模式。
借助Smart ContRaots。

插图。



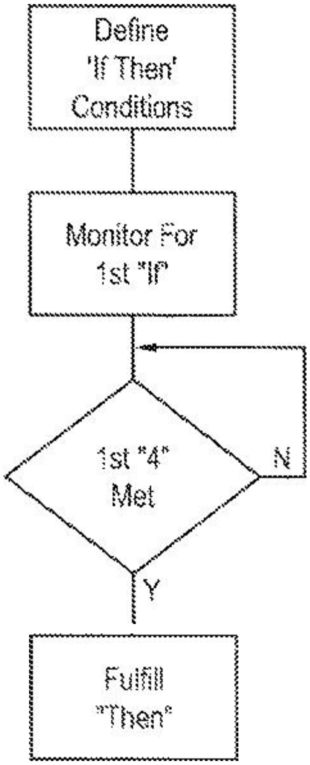
顺序散列 Vsfce Creathn(Hssh VakB Plus Block P^us None»>粉
瞬 r Hash VAhe)

FIG. 19



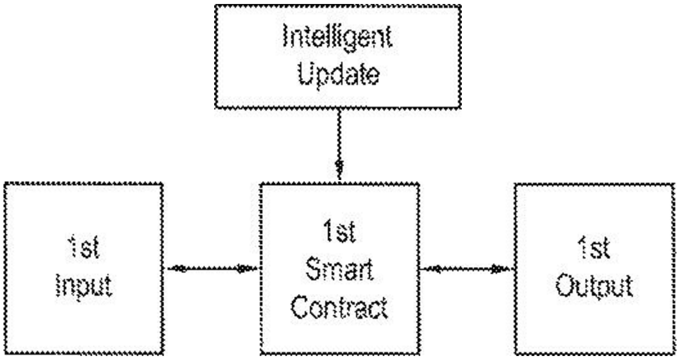
用于加密货币网格的 Ffowchart。

F/G。20

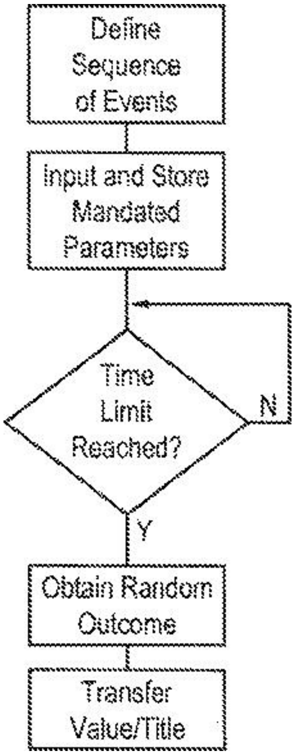


智能契约。

要8S *和*摆的GB ff。



^Smsrt2)合同。



具有强制和Varfeh^参数的智能合同。

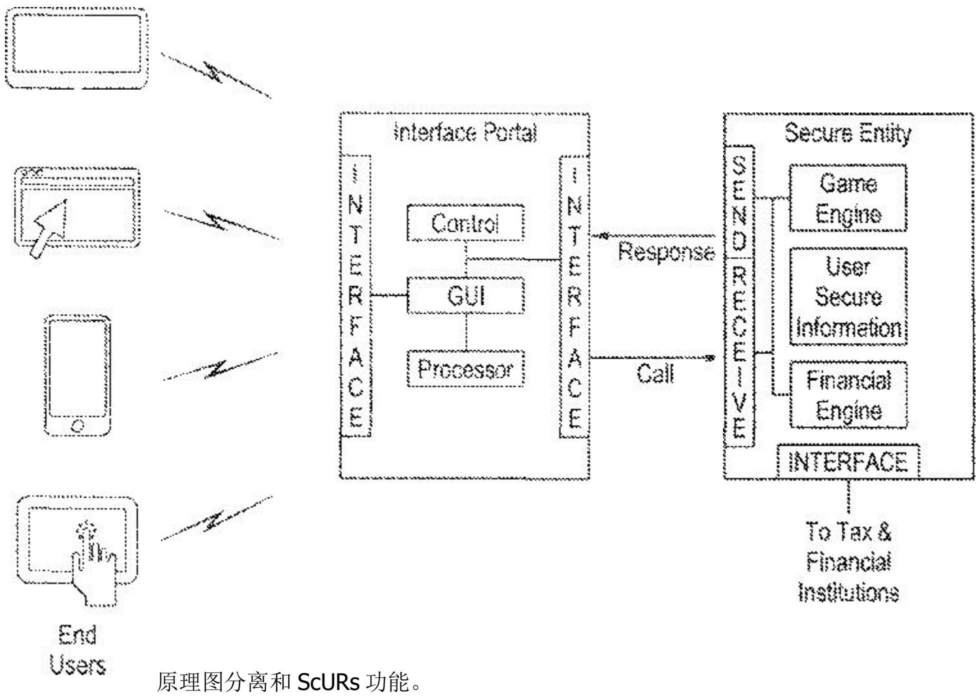
J・W・诳秘 I！&知 d j。

我的账户是托莱。
以太4,328.467。

：Coir。

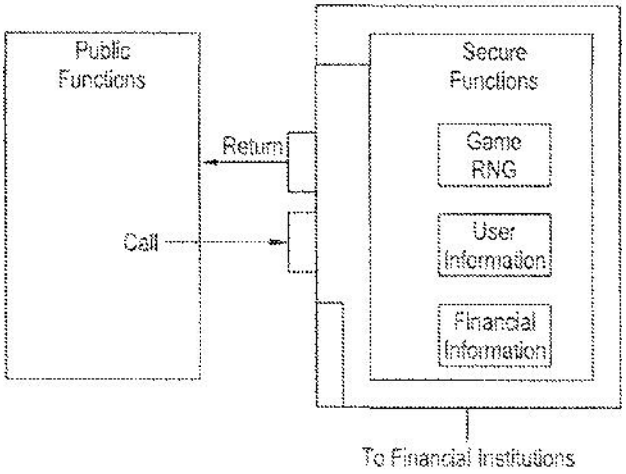
好了！支点。
好了！洛亚希。
我是弗雷奇-兰西。
我是阿瑟；埃斯。
：最新的Tfansacfens。

J-AprH 12。		10
J月30日。	转移X-TwewH VVafets采购(&T)。	0，37枚硬币。
我是2月2日。	奖励帕基尔斯。	11QQ7点。



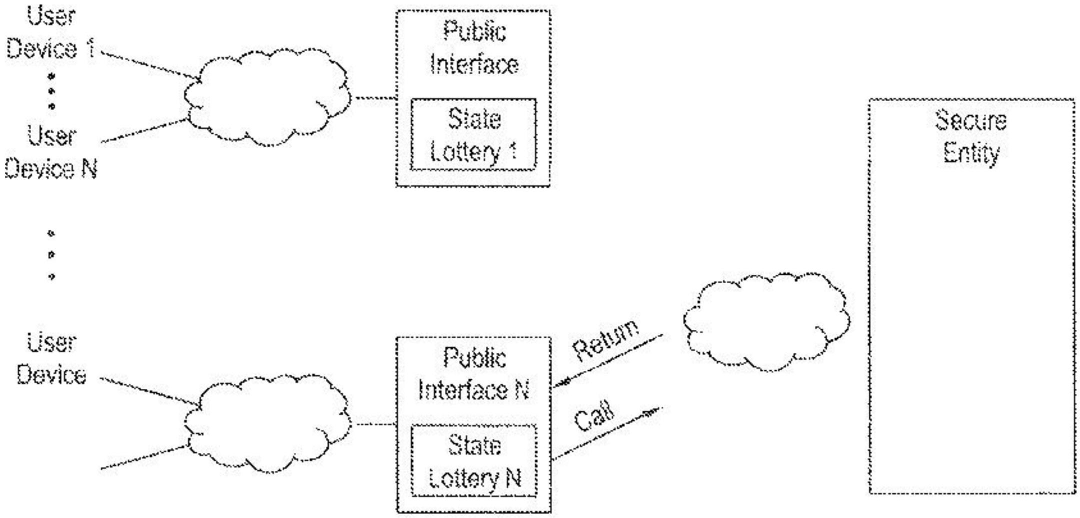
原理图分离和 ScURs 功能。

FIG. 25



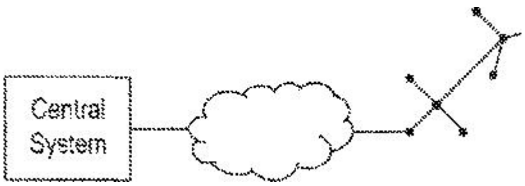
Interface of Segregated Secure and Public Functions

FIG. 26



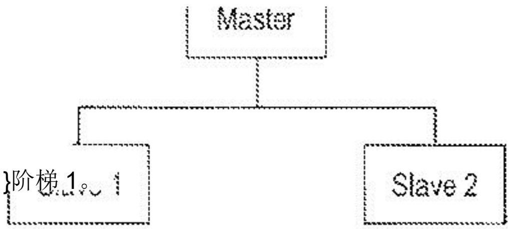
Network Implementation of Segregated Secure and Public Functions

FIG. 27



Centralized + Decentralized Systems

FIG. 28



Hierarchical Systems

FIG. 29

x。

约瑟夫 A.8 恣洪。

07721

LOTIgiy Lbiked CredH 卡。

F/GX 30。

具有分离的安全功能和公共功能的体系结构、系统和方法。

优先权申请。

[0001]这是申请序列号的延续。其要求 2017 年 2 月 3 日提交的临时申请第 62/454,423 号的权益，该临时申请通过引用结合于此，就好像在此完全阐述一样。

本发明的领域。

[0002]本发明涉及用于以编程方式控制的娱乐状态系统的体系结构、系统和方法。更具体地，涉及利用认知计算进行程序控制的体系结构、系统和方法，包括但不限于人工智能和机器学习，并且可选地包括分析。提供了系统、方法和体系结构，利用可选地在对等系统中的包括区块链的分散系统来提供 FBR 游戏和娱乐操作。更具体地说，涉及在分散系统中利用诸如比特币的加密货币实现彩票、游戏或娱乐的系统和方法。

发明背景。

[0003]历史表明，为了提供社会和企业的 FBR 高效运作，许多可信系统已经发展。一般来说，这些都涉及对系统的集中控制，以确保遵守规则。在游戏领域，例子包括彩票和受监管的游戏。例如，内华达州博彩管理委员会监督该州博彩管理机构遵守法律法规的情况，并确保该行业公平和高效地运作。

[0004]考虑一下娱乐和游戏系统背景。彩票是一种“国家”功能，是一种“信任代理”。彩票要素的经典定义是奖金、机会和对价。当这些元素按更正确的时间顺序重新排序时，即首先，收到并持有对价(例如，购票)、机会(例如，确保公平和准确的随机数生成器)和奖品(即，将奖金支付给真正的获胜者)。因此，国家充当一个“信托代理人”，因为它持有对价，保证“4 次机会”的随机性，并支付奖金(所有权转让)。“信任”是建立在系统运营者和监管机构的诚信和可信度的基础上的。彩票或州监管机构往往是前执法人员。对监管机构的信任程度通常基于时间和过往记录，例如，内华达州监管系统被认为是高度值得信赖和有效的，部分是基于数十年的过往记录。此外，在监管过程中失去信任最容易造成企业损失的州最有动力提供监管。这样的系统基于对系统的集中控制。

[0005]赌场是一种四国管制的功能，是一种经过验证的“委托代理”形式。它们由国家颁发许可证，并接受国家检查。

[0006]在游戏和娱乐环境中取得了各种进步。现将以下内容转让给本合同的受让人，特此并入。通过引用好像在此完全阐述：游戏，以及在机会游戏和技能游戏中改进游戏的方法，美国帕特。第 6,565,084 号，游戏，以及 FBR 在机会游戏中的方法和设备，美国 PAT。第 6,488,280 号，游戏，以及 FBR 在机会游戏中的方法和设备，美国 PAT。编号 6,811,484，设备和方法 FBR Game play in a Electronic Environment，U.S.PAT。编号 8,393,946，设备、系统和方法 FBR Implementing Enhanced Gaming and Priking PaRameters in a Electronic Environment(在电子环境中实现增强型游戏和奖励参数的 FBR)，美国专利。编号 7,798,896，设备、系统和方法 FBR Implementing Enhanced Gaming and Priking PaRameters in a Electronic Environment(在电子环境中实施增强型游戏和奖励参数的 FBR)，美国专利。编号 8,241,110，方法和设备 FBR 增强彩票和游戏环境中的游戏，美国专利。No.8,727,853，Methods and Approach FBR Enhanced InteRactive Game Play in Lotting and Gaming Environment。美国帕特。No.8,241,100，Method and System FBR Electronic InteRaction in a Multi-Player Gaming System(多玩家游戏系统中的 FBR 电子交互)，美国专利。8,535,134 号。通常，它们由一套工具组成，以使系统更具吸引力，并优化结果。

[0007]大型系统中的一个令人烦恼的问题是系统不兼容。各种组件通常来自不同的供应商。通常缺乏互操作性和不兼容性。游戏生态系统中的各种系统需要互操作，包括但不限于：游戏运营、营销、CRM(客户关系管理)、忠诚度计划、辅助积分或积分、系统分析和优化以及账户和审计功能。

[0008]软件定义系统是在更高级别的软件控制下互操作的模块集合。它们通过抽象较低级别的功能来管理网络服务。一般来说，存在应用平面、控制平面和数据平面。示例包括具有控制平面的软件定义网络，该控制平面提供对由相对较不智能的交换机、路由器、存储器组成的数据平面的智能控制。另一个例子是软件定义的无线电。控制平面监视和监督数据平面中频段的使用。

[0009]另一个组件是使用静态接口和工具。例如，API 或应用编程接口通常包括静态接口。它们定义了信息请求的格式 FBR。“如果你以特定的方式询问 FBR X，我们会提供 Y‘。一般情况下，除了通过 API，请求者不会提供对系统的访问。还有一个系统是 SDK，即软件开发工具包(Software Development Kit)。它们可能是静态的。提供了实现预期结果的工具。GDK 或游戏开发工具包也可以是静态的，并提供 FBR 游戏开发工具。

[0010]娱乐或游戏的设计通常由度量驱动的设计驱动。这通常涉及 A/B 测试，比较多个系统之间的结果或优惠度。此外，他们经常监测多变量反应系统。

[0011]彩票和乐透风格游戏的一个方面是它们往往是静态的。在最极端的例子中，它们是字面上印在纸板上的。更一般地，一旦彩票游戏选择了一种格式，例如 49 种格式中的 6 种，就很难改变。公众对变化的看法是，这个游戏对玩家变得不那么有利了。

[0012]赌博问题一直困扰着博彩业。这是 FBR 社会的一个重大问题。而用户可以。

在寻求帮助(例如，1-800-赌博)的情况下，通常会有拒绝和不愿意寻求帮助的情况。已经进行了各种尝试来限制滥用，例如在一些在线游戏中使用速率限制。

[0013]在从实体领域向在线和网络领域转移的过程中，身份问题激增。问题包括：你是你声称的那个人吗？用户的身份会被泄露吗？

[0014]认知智能和适应性智能取得了重大进展。例如，IBM Watson 在 2011 年与高技能选手举行的“危险边缘”(Jeopardy)比赛中获胜。深度学习和模式识别已经出现。目前的趋势包括大数据、模式识别和机器学习。

[0015]在 2D 和 3D 空间中的目标检测方面也取得了最新进展。大规模视觉识别挑战赛(LSVRC)中的一项挑战在 ImageNet 2016 中提供了 FBR 对象检测。ImageNet 的自动标签错误率降至不到 3%，而人工操作的错误率约为 5%。

[0016]在基于机器的游戏性能方面也取得了重大进展。2015 年，Google Deep Mind 使用人工智能强化学习系统学习如何玩 49 款雅达利游戏。2016 年，谷歌的 AlphaGo 系统以 4：1 击败了世界上最伟大的围棋选手之一。2017 年，卡内基梅隆大学(Carnegie Mellon University)的 LiBRatus 项目以统计意义上的方式击败了顶级人类选手。

[0017]在基于云的系统方面取得了进一步的进展。功能已经从本地服务器和存储迁移到远程“云”存储。这些系统提供了 FBR 轻松的可扩展性。基于云的系统可以同时运行多个 4个实例。他们还可以结合软件即服务，包括人工智能(“Al”)。

[0018]物联网(IoT)利用能够向远程位置发送数据和接收命令数据的设备。各种语音控制设备使用人工智能或机器学习(ML)，例如 AmAzon Alexa、Google Dot。**[0019]图 1.。1** 示出了示例性的现有技术集中系统。插图。**2** 示出了示例性的现有技术分布式系统。

[0020]在可信分布式系统中取得了进步，例如在使用基于区块链的系统方面。区块链技术的最初披露归功于中本聪(Satoshi Nakamoto)在 2008 年 10 月发表的一篇论文。该系统提供 FBR 自动信任或系统信任。区块链范式为 FBR 提供了一个利用分散共识的分散系统。这可以在没有中介的情况下以点对点的方式完成。该系统可以被视为在可编程分布式网络上运行软件的节点网络。它有时被称为具有共享状态事务单例机器、基于事务的状态机、消息传递框架、可信对象消息传递计算框架和可信计算。

[0021]区块链和密码学的结合建立了分散共识。权威和信任由分散的虚拟网络提供。共识逻辑通常与应用程序分开。它可以包括分散架构的第一层。

[0022]区块链使用分布式分类帐。“块”由一组新的已接受事务组成。在一个块中释放一批事务，以供。参与的计算机网络。公共区块上连续的、顺序的交易记录创建了唯一的“链”或区块链。此块将发布到所有其他节点。该出版物定期发布，例如每 10 分钟发布一次。

[0023]EtheriUm 是一个开源的 FBR 智能合约平台。就目前的运营而言，EtheriUm 是一个运行智能合同的去中心化平台：应用程序完全按照程序运行，没有任何停机、审查、欺诈或第三方干扰的可能性。这些应用程序运行在定制的区块链上，这是一种极其强大的共享全球基础设施，可以移动价值并代表财产的所有权。这允许开发商根据长期的指示(如遗嘱或期货合约)创建市场、存储债务或承诺记录、转移资金，而不存在交易对手风险。EtheriUm 还表示，其目标是创建一种可交易的数字令牌，可以用作货币、资产的表示、虚拟份额、成员资格证明或任何东西。这些代币使用标准的硬币 API，因此合同将自动与任何钱包、也使用此标准的其他合同或交易所兼容。流通中的令牌总量可以设置为简单的固定量，也可以根据任何编程规则集进行浮动。总而言之，EtheriUm 表示，它可以建立一个固定供应的可交易令牌，一个可以发行货币的中央银行，以及一种基于谜题的加密货币。

[0024]当前的系统有许多缺点。他们改变和创新的速度很慢。它们通常涉及不能互操作的专有系统。这往往存在政府和/或体制上的偏见。可能会有一个繁琐的监管环境。最后，交易成本往往很高。

[0025]因此，需要在不一致的、通常是专有的系统之间进行 FBR 互操作性。有必要在更全球化的基础上限制 FBR 赌博，包括地理模拟和全球使用率监测 FBR 问题赌博。有必要对 FBR 问题进行赌博检测和补救。因此，需要对分布式系统进行 FBR 改进。

发明内容。

[0026]一方面，本发明包括娱乐状态系统的系统 FBR 控制，该系统具有由系统的一个或多个用户使用的分离的安全功能和公共功能 FBR。首先，公共接口门户从一个或多个用户接收关于娱乐状态系统的操作的指令。所述接口门户包括：第一接口，用于从所述一个或多个终端用户接收指令并与所述一个或多个终端用户通信；处理器，耦合到所述处理器的图形用户界面(GUI)；与所述处理器和图形用户界面进行操作通信的控制单元；以及提供应用程序接口(API)的第二接口。其次，提供安全实体单元，该安全实体单元包括接收接口、适于从接口门户的应用程序接口(API)接收调用的接收接口、发送接口、适于提供对接口门户接口的响应的发送接口、游戏引擎和金融引擎。优选地，金融引擎耦合到游戏引擎、接收接口和发送接口。

[0027]提供了 FBR 训练人工智能系统的系统和方法，该系统和方法包括使用一个或多个人类主体对刺激的反应作为。

人工智能系统。一个或多个显示器朝向人类受试者以向人类受试者呈现刺激。一个或多个检测器用于监视人类受试者对刺激的反应，所述检测器至少包括运动检测器，所述检测器提供输出。耦合分析系统以接收检测器的输出，该分析系统提供对应于人类受试者的反应是阳性还是阴性的输出。当分析系统的输出为正时，神经网络利用分析系统的输出为神经网络的训练提供正权重，当分析系统的输出为负时，神经网络为神经网络的训练提供负权重。

附图的简要说明。

[0028]图 3.。1 是现有技术集中式系统的示意图。

[0029]图 3.。2 是现有技术集中系统的示意图。

[0030]图 3.。3 是显示应用平面、控制平面和状态数据平面的程序定义娱乐状态系统(PD-ESS)的系统级框图。

[0031]图 3.。4 是 PD-ESS 的应用状态平面层的系统级框图爆炸。

[0032]图 3.。5 是 PD-ESS 控制平面层的系统级框图爆炸。

[0033]图 3.。6 是 PD-ESS 的状态数据平面层的系统级框图爆炸。

[0034]图 3.。7 是生态系统的图解视图，包括接口和互连。

[0035]图 3.。8 是包括图形处理单元(GPU)的神经网络模型体系结构的系统级框图。

[0036]图 3.。9 是神经网络模型体系结构的系统级框图。

[0037]图 3.。10 是包括差异引擎和数据分析器的多个数据集的系统级图。

[0038]图 3.。11 是响应系统显示和检测系统，用于生成训练人工智能(AI)和机器学习(ML)系统的输入。

[0039]图 3.。12 是动态系统应用编程接口(D-API)的系统级图。

[0040]图 4.。13 是动态软件开发工具包(d-SDK)的系统级图。

[0041]图 4.。14 是包括区块链和以太网的分布式系统的系统架构层级图。

[0042]图 4.。15 是允许的区块链系统的系统架构层级图。

[0043]图 3.。16 是区块链平台的系统架构层级图。

[0044]图 3.。17 是包含开链服务的区块链平台的系统架构层级图。

[0045]图 3.。18 是具有智能合约的去中心化加密货币系统的系统架构层级图。[0046]图 4.。19 是具有顺序散列值创建的分散系统的系统体系结构层级图。[0047]图 3.。20 是加密货币彩票的流程图。

[0048]图 3.。21 是智能合约的流程图。[0049]图 3.。22 是智能-智能(Smart2)合同的流程图。

[0050]图 3.。23 是具有强制和可变参数的智能合同的流程图。

[0051]图 3.24 是加密货币钱包的图形用户界面(GUI)。

[0052]图 3.。25 是具有分离的公共和安全功能的系统的系统体系结构级示意图。

[0053]图 3.。26 是分离的公共和安全功能的接口的系统体系结构级别。

[0054]图 3.。27 是具有分离的公共和安全功能的系统的网络实现的系统体系结构级别。

[0055]图 3.。28 是集中式和分散式相结合的系统架构层。

[0056]图 3.。29 是分层系统的系统架构级别。

[0057]图 3.。30 是彩票关联信用卡的平面图。

本发明的详细描述。

[0058]用于节目定义的娱乐状态系统的体系结构、系统和方法。

[0059]下面的描述主要结合图 6。3、4、5 和 6，但也可适用于其他数字。提供了一种体系结构，该体系结构是节目定义的娱乐状态系统。这优选地用于将控制整体体验的系统与定义状态的底层系统分离。第一平面即应用平面提供接口，主要是 FBR 系统侧用户，例如事件、竞赛、彩票的组织者、开发者。第二个平面，控制平面，提供 FBR 智能控制，特别是认知计算，包括人工智能和/或机器学习，包括系统随着时间学习的人工智能。这优选地在模块之上提供智能控制层。第三平面，即状态数据平面，为 FBR 娱乐 4 状^{态}模块提供各种机制，优选地包括“核心环路”、元状态，并提供接口 FBR 终端用户以及输入和输出。

[0060]图 3.。3 提供了框图程序定义的娱乐状态系统(PD-ESS)。插图。4 是 PD-ESS 应用平面层的爆炸式增长，包括应用层 GUI(面向开发人员、分支机构和慈善机构)。插图。5 提供爆炸 PD-ESS 控制器平面层。插图。6 提供爆炸 PD-ESS 状态数据平面层。还包括娱乐状态网元层的爆炸性增长、用户界面 GUI、价值/所有权转移网元的爆炸性增长以及其他功能块的爆炸性增长。

[0061]首先转到应用平面层，程序用于向 PD-ESS 控制器传达要求和期望的行为。它通过 PD-ESS 应用控制器接口(ACI)提供 PD-ESS 应用和 PD-ESS 控制器之间的通信。可选地提供应用程序逻辑和驱动程序。应用层可以接收状态数据平面动作的抽象视图。PD-ESS 应用程序可以与更高级别的抽象控制接口。该系统包括一个接口，即 PD-ESS 应用控制器接口(ACI)。优选地，该管理和管理提供以下内容：(1)到/从应用平面，它提供合同和 SLA，(2)到/从控制。

平面配置策略、监视性能和(3)数据平面元素设置。

[0062]第二转到控制平面层，PD-ESS 控制器在理想的逻辑上是集中式实体，优选地用于将 PD-ESS 应用的要求转换到状态数据平面层，并向应用层提供状态数据平面中的动作(例如，事件信息和统计信息)。控制平面可以从数据平面向应用平面提供统计数据、事件和状态。控制平面优选地在数据平面中的低级控制处实施行为，提供能力发现，并监视统计数据和故障。控制平面有利地包括认知计算，诸如人工智能(Al)和机器学习(ML)，下面将更详细地描述。

[0063]控制平面可以可选地包括分析，包括但不限于模式识别。可以对群体(最好是相关群体)或子集执行分析。优选地，该子集具有与目标用户相似的特征。数据可以根据子集入库。可以分析原始数据的范围。可以包括预测建模。可以在控制平面级别实施负责任的游戏控制，特别是在存在使用率限制和全局限制的情况下。

[0064]第三，转向状态数据平面层，其优选地包括主要子组件和功能网元。可选地，功能网元包括以下部分或全部：1.。娱乐状态网元，2.。价值/所有权转让网元，3.。游戏库，如赌场，VET，电子游戏，锦标赛，有奖游乐设施(AWP)，游戏机制，核心循环，技能，揭秘技能，第二次机会，社交，游戏化，奖品，vGLEP 和奖牌，4.。系统、市场营销、促销、CRM、运营、物流、互动、移动/应用程序和响应性设计，5.。站台，6.。频道，7。彩票，包括零售和中央系统，8。忠诚度，9.。负责任的游戏控制，可选地包括使用速率限制和全局限制(也可以在控制平面层中进行)，10.。体育，包括现实世界、梦幻和电子竞技，11 分。Other Live Data Entertainment，12。网络，包括网络通信和网络服务以及 13。管理，包括记录、玩家账户管理、报告、合规性(包括法规遵从性)、安全(包括网络安全、欺诈和风险管理，最好包括审计和支付)。

[0065]娱乐状态网元提供与系统用户的接口 FBR 交互。输入从用户选择接收信息。传感器可以是各种形式，包括声音传感器、运动传感器，无论是 2-D 还是 3-D，例如包括微软 Kinect 系统。“内部数据”主要由与游戏操作相关的数据组成。“要与主数据源组合的 ExtemaF 数据源。这些可能包括 1 个。位置，2。当前活动，如驾驶(由车辆提供，由跟踪电话提供)或锻炼(由 FitBit 或类似工具提供)，3.。经济状况，4.。天气，5。最近的事件/新闻，例如，最近的一次大型强力球胜利，6.。营销信息，7.电子邮件扫描，例如，谷歌扫描 Gmail FBR 内容，8.。社交媒体，以及 9.物联网(LOT)。物联网(LOT)提供了各种形式的互联设备，如数据传感器。传感器产生数据输入“刺激”到系统。通过利用任何形式的输入，该系统能够提供 FBR 大规模并行性。对系统的所有数据“刺激”允许系统对所有数据刺激进行自适应和反应。

[0066]输出为用户提供刺激。表单可能包括：1.图像，例如在显示器上，或通过 GUI 或 VR 系统、AR 系统，2.。具有远程计算能力的瘦客户机显示器，3.投影和全息图，4.声音，5.触觉刺激，6.嗅觉刺激，或 7.神经或其他直接电刺激。

[0067]价值/所有权转移网元用于接收和转移价值(货币、硬币和其他有价物品)。价值可以指可替代的流动资产或其他价值储存。所有权一般指不动产、动产或虚拟财产的所有权。下面详细讨论了区块链、无信任和加密货币系统。

[0068]人工智能(AI)广泛地说是计算机科学中处理智能行为自动化分支。它们是系统，其目标是使用机器来模拟和模拟人类的智能和相应的行为。这可以采取多种形式，包括符号或符号操作 Al。它可以解决分析抽象符号和/或人类可读符号的问题。它可以在数据或其他信息或刺激之间形成抽象连接。它可能会形成合乎逻辑的结论。人工智能是机器、程序或软件所展示的智能。它被定义为智能 Agent 的研究和设计，其中智能 Agent 是一个感知环境并采取行动最大化成功机会的系统。还有一些人将其定义为制造智能机器的科学和工程。

[0069]人工智能通常涉及到神经网络的使用。在各种实施例中，使用神经网络节点的多层堆栈。最低层由颗粒状元素组成。作为游戏应用中的示例，按照更高级别理解的顺序，级别将从单个动作的实例(粒度)、核心循环检测、会话播放、到多会话播放进行。可选地，解析引擎用于将较大的集合(例如数据集或图像)分解或细分为更离散或更细粒度的元素。

[0070]Al 可以具有各种属性。它可能有演绎、推理和问题解决。它可能包括知识表示或学习。系统可以执行自然语言处理(通信)。还有一些人执行感知、运动检测和信息处理。在更高的抽象层次上，它可能会产生社交智力、创造力和一般智力。采用了多种方法，包括控制论和脑模拟、符号、次符号和统计学，以及整合这些方法。

[0071]可以单独或组合使用各种工具。它们包括搜索和优化、逻辑学、概率方法、FBR 不确定性推理、分类器和统计学习方法、神经网络、深度前馈神经网络、深度递归神经网络、深度学习、控制理论和语言。

[0072]Al 有利地在其体系结构中利用并行处理，甚至大规模并行处理。图形处理单元(GPU)提供 FBR 并行处理。当前版本的 GPU 可从各种来源获得，例如 NVIDIA、Nervana Systems。

[0073]机器学习被定义为从经验中构建知识的系统。机器学习用于发现模式和规律。

[0074]深度学习使用神经智能。它易于扩展，通常涉及更多层或神经网络(NN)。神经网络可以有多种形式，包括：有效神经网络、矢量化神经网络、矢量化 Logistic 回归、矢量化 Logistic 回归梯度输出、二分类、Logistic 回归、Logistic 回归代价函数、梯度下降、导数、计算图和 Logistic 回归梯度下降。

[0075]深度神经网络(DNN)通常涉及超参数调整。通常，它们利用正则化和最优化。有时它们被称为深度信念网络(DBN)。

[0076]其他形式的神经网络包括卷积神经网络(CNN)或递归神经网络(RNN)。可用系统的示例包括：LSTM、Adam、Caffe、Dropout、Batch Norm、Xavier/He、Python、Scikit-Leam 和 TensorFlow。

[0077]A1 可以对各种形式的数据集进行操作。数据集可以包括图像，无论是视频图像、2D 数据和/或 3D 数据。可以分析顺序数据。示例包括但不限于自然语言、音频、自动驾驶决策、游戏状态和游戏决策。

[0078]各种工业应用有利地受益于铝的应用。它们包括成像和目标检测，用于识别、分类、挖掘和可选地提供情感分析。其他应用包括自动驾驶。然而，其他应用包括机器人和机器人技术。在医疗保健领域，功能包括成像分析、诊断和游戏化。可以增强各种形式的顺序数据分析，例如语音识别和自然语言处理。音乐应用包括识别和合成。在游戏领域内，应用包括游戏状态序列检测、分析、编队、组合优化和游戏优化。聊天机器人和机器翻译有利地使用了这些系统。

[0079]图 3.。**7** 显示了娱乐或游戏生态系统内的组成功能块。附属公司的作用是获得客户。附属公司收取佣金，例如根据获得的用户数量或收入的百分比(%)。可选地，存在到信用卡功能的链接(将在下面结合图进行讨论。**30)。**

[0080]接下来是计划举办彩票、游戏或其他娱乐活动的慈善机构和其他组织。他们提供客户获取服务。他们是活动(游戏、彩票或娱乐)的接受者。他们还收取费用。

[0081]接下来是开发人员，他们提供游戏设计。作为游戏设计的回报，他们获得了多司法管辖区的使用和付费 FBR 的使用。可以提供增强的应用或应用商店，其中可以查看、选择和下载游戏设计。

[0082]接下来，消费者提供注册和标识信息。注册数据可以可选地包括身份、年龄、地址和验证。可选)数据足以使系统符合了解您的客户(KYC)规则，可选级别为。实名认证。这将存储为永久历史记录。客户获得了玩、赢和接受娱乐的机会。

[0083]接下来是监管机构或信任验证代理。他们提供测试、审批、FBR 游戏公平、整体审批，确保合规和安全。系统授予监管者或信任验证代理对每笔交易(分析仪表板)、玩家帐户、参数、奖金金额和支付以及完整历史记录的访问权限。监管机构或信托验证代理机构获得补偿，无论是费用还是交易金额的一定比例。**[0084]接**下来，彩票充当信托代理，并收取交易额的一定比例。可选地，当彩票的历史功能由生态系统内的另一实体执行时，这些功能可以从系统中消除或蒸发。

[0085]无花果。8 和 **9** 涉及 FBR 训练神经网络的学习过程。通过提供重复的输入刺激，然后训练神经网络以提供正确的输出，可以教导系统基于一个或多个输入刺激形成正确的关联输出。在将输入转换为期望输出时，训练可以包括监督学习，例如当目标值和参数被监督时。或者，训练可以是非监督学习，其中系统试图识别输入中具有可识别结构并且可以再现的模式。或者，系统可以使用强化学习，它独立工作(类似于无监督学习)，但根据成功或失败来奖励或惩罚。优选地，强化学习涉及增量改变。在各种训练技术中，可以使用扰动，其中一个或多个输入参数通常以例如小于输入值的 10%、更优选地小于 5%和更优选地小于 3%的扰动量变化，以便监视扰动对输出的影响。在各种训练技术中，可以使用扰动，其中一个或多个输入参数通常以小于输入值的 10%、更优选地小于 5%和更优选地小于 3%的扰动量变化，以便监视扰动对输出的影响。

[0086]超参数和参数可以在 AI 或机器学习系统中使用。模型参数是根据数据自动估计的。可以根据数据估计模型内部的配置变量。这可能是模型在进行预测时所要求的。值定义了模型的技能。它们可以通过数据进行估计或学习。

[0087]超级参数是手动设置的，并在流程中用于帮助估计参数。使用模型外部的配置变量。一般来说，它不能从数据中估计出来。它们经常用于估计模型参数的过程中。它们通常由系统用户指定。通常可以使用试探法设置超参数。它们经常被调整为 FBR，这是一个给定的预测建模问题。超级分类帐可以用作超级分类帐编写器或超级分类帐结构。

[0088]可以在各种类型的硬件上执行人工智能或机器学习。有利的是，支持并行处理的系统可以提供 FBR 计算速度和效率。NVIDIA 和 AMD 提供图形处理单元(GPU)等并行处理单元。麒麟 970、Apple All 和高通 ZEROTH 处理器均配备神经处理单元(NPU)。人工智能和机器学习处理也可以作为云人工智能或机器学习系统提供，如 Google 和 AmAzon Web Services 提供的。

[0089]图 3.。10 描述了域转换和差异引擎。一个有利的域变换涉及时域到频域(时间序列到频域)。傅立叶级数就是一个例子，它通常用于重复信号，例如振荡系统。傅立叶变换通常用于非重复信号，例如瞬变信号。可以使用诸如快速傅立叶变换(FFT)之类的增强计算技术来提高 FBR 效率和计算速度。另一种域变换是拉普拉斯变换，通常用于电子电路和控制系统。另一种是 Z 变换，通常用于离散时间信号。可以有利地使用数字信号处理器(DSP)。谱密度估计可能包括小波分析、图像分析、数据压缩和多变量分析。有利地使用相关数据集。

[0090]可以使用区分引擎来识别两组或更多组数据之间的区别。该差别可以是基于时间的，例如其中一个数据集与时间 0 有关，而另一组与时间 1、时间 2、时间 3、…、时间 N 有关。可以计算图像中的差别。

[0091]图 3.。11 示出了一个系统，在该系统中，可以监视、捕获和分析受试者的反应，然后将其用作 A1 的输入。在各种努力中，例如在游戏或娱乐设计和创作中，可以监视、分析和使用目标受众的反应来训练人工智能或机器学习系统。受试者对娱乐/游戏刺激的反应用来测量受试者所经历的‘乐趣’，然后该测量(‘FIM’)被用作 A1 或 ML 系统的训练输入。该系统可以检测个体主体行为。或者，该系统可以监视群体行为，用于检测“有趣”的体验，但也可以测量群体或人群的属性，例如兴奋、参与度或基于群体的行为。

[0092]提供显示器作为对一个或多个对象的刺激。可以使用平板显示器或监视器。可选地，可以利用个人观看设备，诸如单独的屏幕、虚拟现实耳机、增强现实设备、平视显示器、投影设备或成像技术。

[0093]利用各种检测器来监视一个或多个受试者的反应。运动检测利用运动跟踪硬件和软件。一台照相机拍摄被摄体的图像。各种摄像头包括微软 Kinect、2D 传感器和摄像头以及 3D 传感器和摄像头。度量检测器可以分析身体部位的位置，例如肢体、关节或面部特征。它可以测量速度、运动、位置或运动的更高级别的导数，如变化率。面部探测器监控 FBR 面部识别。可以检测面部属性，例如正面属性(例如，微笑)或负面属性(例如，皱眉)。可以确定身体位置检测。声音检测可以用麦克风或麦克风阵列来执行。它可以检测声音的属性，例如正面属性(例如，欢呼声)和负面属性(例如，咒骂和嘘声)。利用生物测定扫描检测。生理反应检测可选择性地监测受试者的心率、血压、瞳孔扩张、体温、心电图和精神活动。活动监控检测器监控参与响应，最好包括下注率、参与时间。显示、保留率、重复率和再参与率。有利地利用了分析。

[0094]系统的输出用作人工智能或机器学习系统的输入。例如，在神经网络中使用强化学习的训练中，正权重使用 FBR 正属性，负权重使用 FBR 负属性。

[0095]该系统还可以提供被识别为与成瘾(例如赌博成瘾)相关联的输出，或者与以其他方式对游戏上瘾的对象相关联的输出。当参与程度或轻微上瘾被视为可接受时，可在训练中使用正权重，而当上瘾被视为不可接受或过度时，可在训练中使用负权重。

[0096]人工智能、机器学习、神经网络、在训练 AI/ML 系统中使用用户响应(通常图 2)。**11** 和上面的讨论)可以有利地用于游戏设计和开发、娱乐开发和/或任何创造性开发工作。

[0097]这些系统可以构成工具矩阵。它们可以包括一组给定的工具。从更根本的意义上说，它们包含了一个发现工具的工具。工具可以是游戏状态、娱乐状态或任何形式的状态或物质。

[0098]下面将描述游戏开发，但是工具、系统、方法和架构可以应用于娱乐或任何创造性工作。对于特定的游戏，第一个选项是只提供该特定游戏的基本规则。为了发现获胜的游戏策略，该系统可以与其自身对战，或者与其他系统对战。在另一种选择中，可以向系统提供已知的游戏比特，允许系统使用或忽略游戏比特。在又一备选实施例中，该系统可以配备有游戏库。该系统可以分析游戏库、FBR 游戏元素、游戏机制或核心循环。可选地，系统可以将游戏库的分析限制为类似的游戏，或者可以考虑可选地分成子单元的所有游戏，例如纸牌游戏、棋盘游戏、视频游戏。一旦定义了各种核心循环或游戏元素，系统就可以将它们组合成各种组合和排列，以便定义新的游戏或游戏进行序列。系统可以识别数据中的模式。可以将值分配给各个点或游戏状态或游戏状态决策点的决策。用户响应的使用可以有利地用于游戏形成和优化。用户响应的使用特别适合于强化学习。

[0099]该系统可以以分层方式操作。可以使用分级系统，其中它可以改变一个从属强制参数，只要满足“上级”或“主”强制参数即可。举例来说，可以使用‘超级’强制参数‘来保证特定的结果。可替换地，可以授予管理控制，诸如设置‘top LeveF 约束’。

[0100]系统可以考虑合作动作中的单独功能。职能可能会被重新分配或转移到其他(特别是较低的)行动级别。系统可能会提供新的变量。通过提供分层响应，可以维护核心功能。可选地，该系统可以例如基于来自管理员的命令或基于预定义的标准来使用系统的“终止开关”FBR、凋亡。该系统可以提供。

体验包(“Total RecalF”)，例如处于连续状态和/或持续状态。

[0101]无花果。12 和 13 涉及各种动态的、多变的系统。在名称“d-API”和“d-SDK”中，‘d’代表 4dynamic‘，并且能够在系统内和由系统进行更改。交互(请求和/或响应)的格式可以是改变。或者，它可以改变响应中提供的信息的类型、数量或质量。其他可能更改的因素包括请求通过 API 或 SDK 更改信息的能力。可以更改其他操作或管理权限，例如只读访问、读写、编辑权限、超级管理权限。这些都提供了自适应控制下的 FBR 动态变化。

[0102]在动态应用编程接口(d-API)内，定义初始格式的 FBR 请求和响应。这可以在 tiSThen，语句中考虑'如果您要求 FBR X 采用商定的格式，则系统将提供 X。动态系统可能会改变格式和/或响应。智能动态更新可以基于人工智能、机器学习或分析。虽然不限于以下，但这些改变中的一些或全部可以动态实现：交互的格式(请求和/或响应)、对更多信息或功能的访问(例如只读)或修改权限、向系统提供信息或数据的能力、以及改变数据的能力。

[0103]在动态游戏开发工具包(d-GDK)中，提供了初始工具包。然后，系统允许动态修改 GDK。优选地，动态修改基于人工智能或机器学习或分析。

[0104]可以提供动态隔离彩票(d-SL)，其中可以提供一个或多个功能单元或彩票。可以使用虚拟化系统，例如在使用虚拟化服务器时。

[0105]无花果。14-20 涉及区块链实现 FBR 游戏、娱乐或其他有用的目的。区块链使用加密的“散列”来识别每个区块和交易。每个连续的块都包含先前代码的散列。这将按时间顺序永久修复事务。区块链同时利用私钥和公钥。将先前的散列与现时值一起添加到新的区块链中，以形成新的散列。

[0106]加密货币提供 FBR 加密安全交易。加密货币是一种可编程货币或分散的价值转移系统。它也是一种去中心化的虚拟货币或去中心化的数字货币。

[0107]工作证明或利害关系证明是参与区块链的“权利”。它必须足够繁重，可以在不重做工作的情况下阻止更改。比特币是一种创造的货币，它被挖掘出来，作为一种奖励，用于 FBR 支付处理工作。区块链加密货币不涉及交易手续费或购买者支付的费用。没有退款权利或退款。

[0108]它可以在任何形式的公共和私有网络中实现。可以使用开放软件和专有软件。存储可以是本地存储或云存储和计算。分析可以在本地或在云分析系统中执行。可以执行分析即服务(AAAS)。系统可以是许可的，而不是无许可的分布式系统。

[0109]无花果。21 至 23 与智能合约有关。核心要素是，第一，一套承诺，可以是合同的，也可以是非合同的。其次，它们以数字形式指定，以电子方式运行，其中合同条款或功能成果嵌入代码中。第三，它们包括基于协议或技术的基于规则的操作。第四，当事人通过自动履行承诺，以一般不可撤销的方式履行承诺。

[0110]智能合同可自动执行不同的流程和操作。在一个实施例中，它们在具有终止性自动执行的基础上自动执行 4iSthis-Then-Then。他们可能会提供 FBR 付款。行动可以以一笔或多笔付款为条件，例如根据付款控制抵押品。

[0111]智能合同可以通过区块链实现。这形成了可在企业对企业实现(B 到 B)和/或对等实现中实现的可信系统。机器对机器的实现允许各种组合。在一个实现中，区块链与构成物联网(LOT)的设备相结合。在另一种组合中，区块链可以与构成物联网的设备与人工智能相结合。通常，该块包含智能合约程序逻辑。它将与特定智能合同相关的消息捆绑在一起，包括输入、输出和逻辑。在又一实施方式中，它们可以提供合约 FBR 差异，例如在使用当前市场价格来调整余额和分散现金流时。

[0112]智能合约是一种信任转移技术。它们降低了交易对手的风险。最好是，这有助于增加信贷。

[0113]智能合同可以在各种模型中实施。它们可能是一份完全用代码写成的合同。它们可以是具有单独自然语言版本的代码中的合同。它们可以是具有编码性能的分裂的自然语言契约。或者，它们可以是具有编码支付机制的自然语言合同。

[0114]智能合同启动需要达成共识。算法构成合同中的每个参与者如何处理消息的一组规则 FBR。它们可以无许可的方式实现，其中任何人都可以提交消息 FBR 处理。提交者可能参与协商一致。或者，他们可以将决策委托给管理员或参与者子组。另一种实现方式是建立一个允许的系统，其中参与者受到限制。它们通常是预先选定的。然后，他们必须接受门禁进入，并必须满足某些要求和/或管理员的批准。

[0115]智能合同适用于不同的订立方法。他们可以通过协议达成协议，例如在有共同的合作机会或确定的预期结果的情况下。这些可能包括商业惯例、资产互换和权利转让。下一步，条件设置 FBR 合同的启动。这可能是由当事人自己决定的，也可能是由某些外部事件的发生造成的，例如时间、其他可量化的度量或地点。通常，他们会生成一个代码，该代码是用区块链技术加密和链接的。它可以被认证和验证。在执行和处理时，网络更新所有分类帐以指示当前状态。一旦验证并发布，它们就不能更改，只能附加其他块。

[0116]重申一下，智能合同作为具有独立内置信任机制的网络上的分布式应用程序。程序赋予价值单位结合规则 FBR 转让价值单位的所有权。它们充当自动执行程序，自动满足程序化关系的条款。

[0117]图 3.。20 示出了作为智能合约实现的彩票实施例。实现抽奖的方法 FBR 包括以下步骤。设置接收加密货币的时间范围。第二，在时间范围内接收带有所有者标识的加密货币。窗口在指定的持续时间内打开 FBR，之后窗口关闭。智能合约例如从随机数生成器生成或接收随机事件。随机数生成器应该包括随机性的算法保证和无黑客攻击的保证。合同在所有者标识相关的加密货币中选择新的所有者(赢家)。然后，它将加密货币的新所有权分配给选定的新所有者(获胜者)。

[0118]智能合同可用于实现核心循环或游戏机制。以下核心环路和游戏机制包括可实现的部分列表，包括但不限于 Jacko、Poko、hotSeat、Hi Lo、Rock、Paper 剪刀、In The Zone 和 iLotto 或其他基于阵列或地理的游戏机制或核心环路。游戏机械师或核心循环的任何子单元本身都可以用作游戏机械师或核心循环。

[0119]Jacko 是一种游戏，包括以下步骤：从具有最小和最大数字的第一数字范围中随机选择目标数字；向玩家呈现目标数字的指示；选择数字 FBr，该数字从具有最小和最大值的第二范围中选择，其中最大值等于或小于第一范围的最小值的 52；从玩家接收是否再次抽签的指示；如果是，则从第二范围中随机选择一个数字，累加玩家的抽签总数，重复该步骤，直到玩家拒绝抽签或者总数超过目标数目，并且在玩家拒绝抽签的情况下，从第二范围中随机选择数字，累加这些数字，将它们与玩家的累积量进行比较，并且分配总数目最接近但不超过目标的获胜者。

[0120]Poko 是一个多玩家游戏，其中多个标记被授予预定值，而其他玩家没有关于其他玩家持有的至少一些标记的信息。

[0121]高 LO 是一种包括以下步骤的游戏：对一系列随机抽取的数字执行第一次抽奖选择，从玩家接收下一个随机抽取的数字将高于还是低于前一个数字的指示，如果正确，则奖励与随机抽取的数字的数量相关的奖金，并且继续进行，直到玩家无法预测高/低结果，或者选择停止。

[0122]在该区域中是一种碰运气游戏，该游戏包括以下步骤：在预定义的数字范围内随机选择玩家的目标数字，该范围具有最小值和最大值；随机选择彩票游戏中使用的一系列数字 FBR，该预定义数字范围的最小值至少等于最低可能总 FBR 的系列的总和。该数字序列和预定义数字范围的最大值，在选择结束时将随机选择的数字序列合计，并基于玩家数量和总数量的接近度，将奖金金额分配给玩家数量不超过总数的玩家。

[0123]石头布剪刀是一种具有三个或更多选项的游戏，这些选项相对于彼此具有指定的选项优先级。

[0124]竞争席位是一种增加风险/回报的游戏，包括在 Smart ContRact 中选择退出的能力。一种在最终级别达到最终级别的多级机会游戏中进行 FBR 游戏的方法，包括以下步骤：在给定级别呈现多个随机选项，其中至少一个选项是正选项，另一个选项是负选项，以及需要进一步决策的第三选项，接收关于选择多个随机选项中的哪一个的选择，以及如果选择了正选项，则将正选项结果与先前正选项结果累加，但是如果选择了负选项，则累加负选项结果，比较累加结果。以及如果累计次数小于预定次数，则重放相同级别，或者如果累计次数等于预定次数，则终止游戏，并且如果选择了第三选项，则接收关于该决定的选择，尊重上述步骤，直到玩家停止，与发生的预定数量的负面事件或最终级别相关。

[0125]iLotto 是基于网格或地理的系统，包括呈现识别对象的网格的显示器 FBR、接收识别对象的玩家选择的输入 FBR、随机选择获胜识别对象的随机生成器 FBR、以及根据规则向玩家奖励积分的计分系统 FBR，所述规则包括：如果玩家选择的识别对象与获胜的识别对象完全匹配，则第一积分值；如果玩家选择的识别对象与获胜的识别对象具有几何关系，则第二积分值；以及如果玩家选择的识别对象与获胜的识别对象具有几何关系，则第二积分值。

[0126]图 3.。23 涉及执行授权参数和可变参数。强制参数在智能合同中设置。强制参数的示例包括支出百分比和支出金额。可变参数受制于强制参数，提供娱乐选项。

[0127]图 3.。24 描绘了用于电子存储加密货币的钱包。这表示诸如在电话或计算机显示器上的图形用户界面(“GUI”)。各种形式的加密货币可以显示在 GUI 上并存储在钱包中。可以奖励积分，例如 FBR 忠诚度、频率和广播时间。可以列出最近或最近的交易，注明日期、目的和金额。可能会显示总帐户值。

[0128]加密货币系统和智能合约可以与其他系统结合实施。一个额外的系统包括常客或球员的俱乐部系统。它们可能与其他形式的“货币轻量级”相结合，包括微交易和微支付。它们可以与智能资产(即知道其所有者是谁的数字资产或实物)结合使用。数字资产是以数字格式(通常是二进制格式)存在的任何东西，并且有权。

使用。示例包括图像(包括静止图片和视频或动态图像)、可听内容(例如声音、音乐或表演)以及数字文档。所有权通过分布式可信网络控制的财产，例如使用合同的区块链。它们还可以与地理位置结合使用，其中各种组件和建筑组件的物理位置(地理位置)可选地是系统的组件。游戏的地理位置可能会受到限制。该系统可以确保符合数据路由的地理位置。

[0129]无花果。25 至 27 **涉**及具有分离的安全功能和公共功能的系统。这为公共功能和公共实体提供了一个具有多个接口的安全平台。分离的安全功能提供信任代理的功能。安全功能包括以下一项或多项。第一，结果决定。这可能包括使用随机数生成器(RNG)或概率引擎。第二，存储用户或玩家帐户信息。第三，存储货币会计或交易。第四，进行监管和合规接口。第五，开发人员界面等界面。第六，可以提供问答测试、合规性测试和审批等监管职能。

[0130]公共职能包括以下部分或全部。首先，公共系统向安全系统发出‘呼叫’。调用可以通过应用编程接口(API)或 D-API 进行。“open”系统调用调用保护系统 FBR 安全数据。其次，设计器界面用于访问工具、API、开发工具包(DK)和软件开发工具包(SDK)。第三，市场界面充当彩票界面以及可选的应用程序或应用程序商店。第四，操作员接口用于与操作员或组织者(例如慈善机构)对接。它最好服务于出版、营销和销售。第五，用户界面允许注册、播放活动和持久历史记录。

[0131]系统部件可能因功能不同而不同。公共接口和功能优选地包括“开放”平台。这允许 FBR 仲裁并与安全实体达成关于由安全实体执行的游戏操作的协议，例如，支付百分比、可以玩的 vGLEP 和地理位置。安全实体执行安全功能，包括游戏结果、财务事项和安全用户数据。终端用户利用包括但不限于网络、移动应用、移动网络、平板电脑、计算机、支持显示的设备(无线)、零售商处的触摸屏设备(例如，台面游戏)的“频道混合”。私人实体可以施加速率限制并施加负责任的游戏控制。

[0132]无花果。28 和 **29** 描述了混合和分层系统。诸如国营彩票的集中式系统可以与诸如区块链实现的分散式系统相结合。可以在系统内强加分层顺序。在使用强制和可变参数的系统中，可以建立强制参数的分层结构，然后各种可变参数可以服从适当的强制参数。在另一应用中，可以在层次中的较高级别施加全局使用率限制。可以实施分级使用费率限制。系统的各种拓扑结构包括主从式、主从式和循环式。

[0133]图 3.。30 涉及游戏或彩票关联的信用卡和信用卡功能。信用卡和信用功能可以链接到彩票或其他游戏。通过使用信用卡，建立了转换率。例如，FBR 每 100 美元的购买，1 美元的彩票游戏。费率可以是可变的，例如基于机构。在组织或赞助彩票或游戏的慈善组织中，每购买 100 美元，该组织将获得 2 美元的 FBR。也可以执行拆分，例如信用卡所有者在彩票或游戏中每购买 100 美元可获得 1 美元的 FBR，组织可获得 1 美元的 FBR。

[0134]在替代实施例中，移动游戏设备可以通过电缆连接到游戏机，或者直接连接到游戏机的端口，或者经由与游戏机通信的网络连接到游戏机。

[0135]用于根据这里描述的实施例对游戏机和服务器进行编程的软件最初可以存储在诸如 CD 或电子存储设备的 ROM 上。这样的 CD 和设备是其上存储有适当的计算机指令的非暂时性计算机可读介质。该程序也可以通过赌场的网络下载到游戏机上。

[0136]应当理解，这里描述的终端、处理器或计算机可以以多种形式中的任何一种实现，例如机架式计算机、台式计算机、膝上型计算机或平板计算机。此外，计算机可以嵌入通常不被认为是计算机但具有适当处理能力的设备中，该设备包括电子游戏机、网络电视、个人数字助理(PDA)、智能电话或任何其他合适的便携式或固定电子设备。

[0137]此外，计算机可以具有一个或多个输入和输出设备。这些设备尤其可以用来呈现用户界面。可用于提供用户界面的输出设备的示例包括打印机或显示屏、输出的 FBR 可视呈现和输出的扬声器或其他声音生成设备 FBR 可听呈现。可用于用户界面的输入设备的示例包括键盘和诸如鼠标、触摸板和数字化平板的定点设备。作为另一示例，计算机可以通过语音识别或以其他可听格式接收输入信息。

[0138]这样的计算机可以通过任何适当形式的一个或多个网络互连，包括作为局域网或广域网，例如企业网或因特网。这样的网络可以基于任何合适的技术，并且可以根据任何合适的协议操作，并且可以包括无线网络、有线网络或光纤网络。如这里所使用的，术语“在线”指的是这样的联网系统，包括使用例如专用线路、电话线、电缆或 ISDN 线路以及无线传输联网的计算机。在线系统包括使用例如局域网(LAN)、广域网(WAN)、因特网以及上述各种组合的远程计算机。合适的用户设备可以连接到网络 FBR 实例、能够通过网络通信的任何计算设备，诸如台式、膝上型或笔记本计算机、移动站或终端、娱乐设备、与显示设备通信的机顶盒、。

例如电话或智能手机、游戏控制台等无线设备。术语“在线游戏”指的是那些利用这样的网络来允许游戏玩家通过远程和本地的联网或在线系统利用和参与游戏活动的系统和方法。例如，“在线游戏”包括通过互联网上的网站提供的游戏活动。

[0139]此外，这里概述的各种方法或过程可以被编码为可在采用各种操作系统或平台中的任何一种的一个或多个处理器上执行的软件。另外，这样的软件可以使用多种合适的编程语言和/或编程或脚本工具中的任何一种来编写，并且还可以被编译为在框架或虚拟机上执行的可执行机器语言代码或中间代码。

[0140]在这方面，实施例可以提供编码有一个或多个程序的有形、非暂时性计算机可读存储介质(或多个计算机可读存储介质)(例如，计算机存储器、一个或多个软盘、光盘(CD)、光盘、数字视频盘(DVD)、磁带、闪存、现场可编程门阵列或其他半导体器件中的电路配置、或其他非暂时性、有形计算机可读存储介质)，当在一个或多个计算机上执行这些程序时。计算机可读介质或介质可以是可运输的，使得存储在其上的一个或多个程序可以加载到一个或多个不同的计算机或其他处理器上，以实现如上所述的各个方面。如这里所使用的，术语“非暂时性计算机可读存储介质”仅包括可被认为是制品或机器的计算机可读介质，并且不包括暂态信号。在此使用的术语“非暂时性计算机可读存储介质”仅包括可被认为是制品或机器的计算机可读介质，并且不包括暂态信号。

[0141]这里一般意义上使用的术语“程序”或“软件”指的是可用于对计算机或其他处理器编程以实现如上所述的各个方面的任何类型的计算机代码或计算机可执行指令集。另外，应当理解，根据本实施例的一个方面，当执行执行方法的一个或多个计算机程序不需要驻留在单个计算机或处理器上，而是可以以模块化方式分布在多个不同的计算机或处理器之间，以实现在此描述的实施例的各个方面。

[0142]计算机可执行指令可以是由一个或多个计算机或其他设备执行的多种形式，诸如程序模块。通常，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等。通常，在各种实施例中，可以根据需要组合或分布程序模块的功能。

[0143]此外，数据结构可以以任何合适的形式存储在计算机可读介质中。为简单起见，可以将数据结构示为具有通过数据结构中的位置相关的字段。这样的关系同样可以通过为具有计算机可读介质中的位置的字段分配存储来实现，该计算机可读介质传达字段之间的关系。但是，任何。可以使用合适的机制来建立数据结构的字段中的信息之间的关系，包括通过使用指针、标签、地址或在数据元素之间建立关系的其他机制。

[0144]这里描述的实施例的各个方面可以单独使用、组合使用，或者以前述描述的实施例中未具体讨论的各种布置使用，因此这里描述的概念在它们的应用上不限于前述描述或附图中所示的组件的细节和布置。例如，一个实施例中描述的方面可以以任何方式与其他实施例中描述的方面组合。

[0145]此外，这里描述的实施例可以提供一种方法，已经提供了该方法的示例。作为该方法的一部分执行的动作可以以任何合适的方式排序。因此，可以构造以与所示不同的顺序执行动作的实施例，这可以包括同时执行一些动作，即使在说明性实施例中被示为顺序动作。

[0146]虽然已经参考其某些示例性特征描述了实施例，但是本领域技术人员可以对所描述的实施例进行各种修改。这里使用的术语和描述仅用于说明，并不意味着限制。具体地说，尽管已经以示例的方式描述了实施例，但是各种设备将实践在此描述的创造性概念。已经以各种术语描述和公开了实施例，实施例的范围不打算也不应该被认为受其限制，特别是当它们落入这里所附权利要求的广度和范围时，可以由这里的教导建议的其他修改或实施例被特别保留。本领域技术人员将认识到，如以下权利要求及其等价物中定义的那样，这些和其他变体是可能的。尽管出于清楚和理解的目的，通过图示和示例的方式较详细地描述了前述发明，但是根据本发明的教导，本领域的普通技术人员可以很容易地看出，在不背离所附权利要求的精神或范围的情况下，可以对其进行某些改变和修改。

[0147]本说明书中引用的所有出版物和专利在此以引用方式并入，就好像每个单独的出版物或专利被具体地和单独地指示通过引用将其整体并入一样。

参考文献。

[0148]IBM ARM，《2017 物联网商业指数，动态转型》，《经济学人》，智库有限公司 2017，第 1-22 页。

[0149]Crosby 等人的《区块链技术：《超越比特币》，《应用创新评论》，第 2 期，Sutardja Center for EntretreURship&Technology，BerkeLey Engineering，2016 年 6 月，第 1-19 页。

[0150]Fisher，《分散式点对点游戏资产平台，使用智能合同与第三方游戏集成》，2014 年 8 月 4 日，12 页。

[0151]Hinton 等，4《深度信念网的AFast 学习算法》。神经计算，18,1527-1554,2006。

[0152]Jouppi 等人的《张量处理单元 TM 的数据中心内性能分析》，将于 2017 年 6 月 26 日在加拿大多伦多举行的第 44 届国际计算机体系结构研讨会(ISCA)上发表，第 1-17 页。

[0153]LeCun 等人，《深度学习》，《自然》，第 521 卷，2015 年 5 月 28 日，第 436-444 页。

[0154]Marvin，4<区块链 A-Z：关于比特币背后的改变游戏规则的技术，你需要知道的一切“。2016 年 6 月 3 日，9 页。

[0155]Marvin，《区块链：《正在改变世界的无形技术》，2017 年 2 月 6 日，32 页。

[0156]Mougayar，The Business BlockChain，第 6-9 页，128-133 页，由 John WiLey&Sons 出版，新泽西州霍博肯。

[0157]Nakamoto，《比特币--点对点电子现金系统》，2008 页。1-9。

[0158]Ng，44《人工智^{能}现在能做什么，不能做什么》，《哈佛商业评论》，2016 年 11 月 9 日，5 页。

[0159]O‘Dowd 等人，《IBM’s Open Blockchain，Making BlockChain Real for Enterprise》，IBM BlockChain，2016 年 4 月，第 1-20 页。

[0160]Ronan，《深度学习预测 LOTO 数字》，巴黎学院，2016 年 4 月 1 日，第 1-4 页。

[0161]智能合同联盟，“‘智能合同：12 个使用案例 FBR Business and Beyond，A Technology，Legal&Regulatory Information，由智能合同联盟一与德勤(数字商务商会的一个行业倡议)合作编写。2016 年 12 月，第 1-53 页。

[0162]图灵，《计算机器与智能》，思想 49：1950 年，第 433-460 页。

[0163]伍德，《以太：安全分散的通用交易分类账“，宅基地草案，2014 年，第 1-32 页。

[0164]Wu 等人的《Google 的神经机器翻译系统：弥合人与机器翻译之间的鸿沟“，2016 年 10 月 8 日，第 1-23 页。

[0165]Yli-HUUmo 等人，“区块链技术的当前研究在哪里？系统回顾“，2016 年 10 月 3 日，第 1-27 页。

术语表。

[0166]51%攻击：对比特币网络的攻击，允许攻击者创建欺诈性交易，参见 Double Spend。这是可能的，因为控制了比特币网络 50%以上的散列率意味着攻击者可以在计算上胜过所有其他正在挖掘的人。

一个。

[0167]帐户：帐户具有作为以太状态的一部分维护的固有余额和交易计数。它们还具有一些(可能为空)EVM 代码和与其关联的(可能为空)存储状态。虽然是同质的，但区分两种实际类型的帐户是有意义的：具有空的关联 EVM 代码的帐户(因此，帐户余额由某个外部实体控制，如果有的话)和具有非空的关联 EVM 代码的帐户(因此，帐户代表自治对象)。每个帐户都有一个单独的地址来标识它。

[0168]地址：比特币地址用于接收和发送比特币网络上的交易。它包含一个字符串。字母数字字符，但也可以表示为可扫描的二维码。比特币地址也是比特币持有者用来对交易进行数字签名的一对密钥中的公钥(参见公钥)。

[0169]地址：用于标识帐户的代码，例如 160 位代码。

[0170]协议分类帐：协议分类帐是两个或多个当事人用来谈判和达成协议的分布式分类帐。

[0171]空投：一种在人群中分发加密货币的方法，2014 年初首次尝试使用 AURoRaco in(AURoRaco In)。

[0172]算法：在计算或其它解决问题的操作中要遵循的过程或规则，尤指计算机所遵循的过程或规则。

[0173]备用币：作为比特币替代品提供的 FBR 加密货币的统称。莱特币、羽毛币和 PPCoin 都是替代币。

[0174]反洗钱：反洗钱技术被用来阻止人们转换非法获得的资金，使其看起来像是合法赚取的。反洗钱机制本质上可以是法律的或技术的。监管机构经常将 AML 技术应用于比特币交易所。

[0175]App：终端用户可见的应用程序，例如托管在以太浏览器中。

[0176]应用程序接口(API)：组件(通常是软件组件)用作彼此通信的接口的规范。可以包括规范 FBR 例程、数据结构、对象类和变量。

[0177]套利：通过在同一资产价格不同的市场之间进行交易而产生的无风险利润。

[0178]ASIC：专用集成电路是专门为完成单一任务而设计的硅芯片。就比特币而言，它们旨在处理 SHA-256 散列问题，以挖掘新比特币。

[0179]ASIC Miner：一种包含 ASIC 芯片的设备，用于挖掘 FBR 比特币。它们可以是插入背板的电路板、带有 USB 连接器的设备，也可以是包含所有必要软件的独立设备，这些设备通过无线链路或以太网电缆连接到网络。

[0180]ASIC 挖掘：许多矿工购买单独的计算设备，完全搁置了 FBR 挖掘。作为另一种选择，他们也可以得到专用集成电路；这是一种专门设计的计算机芯片，用于执行一种特定的功能，在这种情况下，只有一功能，即挖掘计算。ASIC 降低了 FBR 开采所需的处理能力和能源，并可以通过这种方式帮助降低整个过程的成本。无论专用集成电路一(专用芯片本身的术语)是集成到现有的计算系统中，还是作为独立设备运行，术语“专用集成电路”通常指的是整个系统本身，而不仅仅是芯片。

[0181]非对称密钥算法：这是用于生成公钥和私钥的算法，公钥和私钥是加密货币交易必不可少的唯一代码。在对称密钥算法中，发送方和接收方都拥有相同的密钥；它们可以私密地加密和交换信息，但是由于双方都拥有解码信息，所以它们不能对彼此保密。使用非对称密钥算法，双方都可以访问。

公钥，但只有拥有私钥的人才能解密加密；这确保了只有他们才能收到资金。

[0182]证明台账：一种分布式分类帐，提供协议、承诺或声明的持久记录，提供这些协议、承诺或声明已作出的证据(证明)。

[0183]自治代理：在没有人工干预的情况下做出决策并对其采取行动的软件。

[0184]自治对象：仅存在于假设的以太状态中的虚构物体。有一个内部地址，因此有一个关联的帐户；该帐户将具有非空的关联 EVM 代码。仅作为该帐户的存储状态合并。

B 类。

[0185]基数 58：Base58 将二进制数据编码为文本，并用于编码比特币地址。由中本聪(Satoshi Nakamoto)创作，字母数字字符不包括“0”、“O”、“1”、“I”，因为它们很难区分。

[0186]Base58 检查：Base58 的变体，用于检测比特币地址中的键入错误。

[0187]BIP：“比特币改进建议”的首字母缩写，任何想要改善比特币网络的人都可以提交。

[0188]位：比特币面值的名称，等于 100 Satoshis(1 比特币的百万分之一)。2014 年，包括比特币(Bitpay)和 Coinbase 在内的几家公司以及各种钱包应用程序都采用了 BIT 来显示比特币金额。

[0189]比特币(大写)：众所周知的加密货币，基于 ProoSof-Work 区块链。

[0190]比特币(小写)：比特币账本使用的具体技术集合，一种特殊的解决方案。请注意，货币本身就是这些技术之一，因为它为矿工提供了开采的动力。

[0191]比特币(货币单位)：一亿，000,000 个智士。一种分散的数字货币单位，可以用来交易商品和服务。比特币也是替代货币生态系统中的一种储备货币。

[0192]比特币 2.0：比比特币白皮书提出的基本支付系统应用更高级或更复杂的比特币或区块链技术的 FBR 应用。比特币 2.0 项目的例子包括对手方、以太、Blockstream、Sarm、Domus 和 Hedgy。

[0193]比特币自动取款机：比特币自动取款机是一种实体机器，允许客户用现金购买比特币。有很多制造商，其中一些可以让用户出售比特币 FBR 现金。它们有时也被称为“BTM”或“比特币 AVMS”。CoinDesk 维护着一张运营比特币 ATM 机的全球地图和一份制造商名单。

[0194]比特币核心：自 2014 年 3 月 19 日发布 0.9 版以来，比特币 Qt 的新名称。不要与 2013 年 8 月发布的 Objective-C 实现 Core 比特币混淆。

[0195]Bitcoind：使用命令行界面的比特币的原始实现。目前是 BitcoinQt 项目的一部分。根据 UNIX 传统，“D”代表 FBR“守护进程”，用于命名后台运行的进程。

[0196]比特币销毁天数：一个估计 FBR 的“货币的速度，与比特币网络。之所以使用这种方法，是因为它赋予了尚未使用的比特币更大的权重。FBR 花费了很长时间，比起每天的总交易量，它更好地代表了使用比特币进行的经济活动的水平。

[0197]比特币投资信托基金：这一私人的开放式信托专门投资于比特币，并代表其股东使用最先进的协议来安全地存储比特币。它为 FBR 的人们提供了一种投资比特币的方式，而不必自己购买和安全地存储这种数字货币。

[0198]比特币 J：迈克·赫恩的完整比特币节点的 Java 实现。除其他功能外，还包括 SPV 实现。

[0199]BitcoinJS：一个在线的 javascript 代码库使用了 FBR 比特币开发，特别是网络钱包、比特币游戏。O 昭(网址：“BitcoinJ s.org)。

[0200]比特币市场潜力指数(BMPI)：比特币市场潜力指数(BMPI)使用一个数据集对 177 个国家的比特币潜在效用进行排名。它试图展示哪些市场最有潜力采用 FBR 比特币。

[0201]比特币网络：维护区块链的分散的点对点网络。这是处理所有比特币交易的工具。

[0202]比特币价格指数(BPI)：CoinDesk 比特币价格指数代表了符合 BPI 指定标准的全球领先交易所的比特币价格平均值。还有一个 API FBR 开发者可以使用。

我们声称：

1. 一种娱乐状态系统的系统 FBR 控制，其具有由系统的一个或多个用户使用的分离的安全功能和公共功能 FBR，包括：

公共界面门户，所述界面门户适于从所述一个或多个用户接收关于所述娱乐状态系统的操作的指令，所述界面门户包括：

第一接口，用于从所述一个或多个终端用户接收指令并与所述一个或多个终端用户通信，

处理器，

耦合到处理器的图形用户界面(GUI)，

与处理器和图形用户界面进行操作通信的控制单元，以及。

提供应用程序接口(API)的第二接口，以及。

安全实体单元，所述安全实体单元包括：

接收接口，该接收接口适于从接口门户的应用程序接口(API)接收调用，

发送接口，所述发送接口适于向所述接口门户接口提供响应，

游戏引擎，

金融引擎，所述金融引擎耦合到所述游戏引擎，以及所述接收接口和发送接口，

以及提供财务信息的接口。

2. 如权利要求 1 所述的系统，其特征在于，所述安全实体还包括用于存储用户安全信息的存储器。

3. 该系统 FBR 如权利要求 1 所述的娱乐状态系统的控制，其中所述财务信息是税收信息。

4. 根据权利要求 1 所述的系统 FBR，其特征在于，所述金融信息耦合到金融机构。

5. 根据权利要求 1 所述的娱乐状态系统的控制系统，其中所述游戏引擎包括游戏随机数生成器(RN)。

6. 根据权利要求 1 所述的娱乐状态系统的控制系统，其中所述安全实体还包括自适应控制单元。

7. 根据权利要求 6 所述的娱乐状态系统的控制系统，其中所述自适应控制单元包括认知计算单元。

8. 如权利要求 6 所述的娱乐状态系统的系统 FBR 控制，其中自适应控制单元包括人工智能单元。

9. 如权利要求 1 所述的娱乐状态系统的系统 FBR 控制，其中所述自适应控制单元包括机器学习单元。

10. 如权利要求 1 所述的娱乐状态系统的系统 FBR 控制，其中自适应控制单元包括神经网络。

11. 如权利要求 10 所述的娱乐状态系统的系统 FBR 控制，其中所述神经网络是深度神经网络。

12. 如权利要求 10 所述的娱乐状态系统的系统 FBR 控制，其中所述神经网络包括图形处理单元(GPU)。

13. 如权利要求 10 所述的娱乐状态系统的系统 FBR 控制，其中所述神经网络是利用用户响应数据来训练的。

14. 如权利要求 10 所述的娱乐状态系统的系统 FBR 控制，其中所述神经网络是矢量化神经网络。

15. 如权利要求 10 所述的娱乐状态系统的系统 FBR 控制，其中所述神经网络是递归神经网络。

16. 如权利要求 1 所述的娱乐状态系统的系统 FBR 控制，其中所述安全实体包括分析单元。

(19)美国。

(12)专利**申请公开(10)。编号：美国 2018 年/0247191 Al。**

Katz et al。　　　　(43)酒吧。**日期：　　2018年8月30日。**

(54)**架构、系统和。**
用于节目定义的娱乐状态系统的方法、去中心化加密货币系统以及安全功能和公共功能分离的系统。

(71)　申请人：**里程碑式的娱乐。**
有限责任公司，加利福尼亚州贝弗利山庄
(美国)。

(72)　发明者：**兰德尔·M·卡茨(Randall M.Katz)，加利福尼亚州贝**弗利山。
(美国)；罗伯**特·特切克(Robert Tercek)，**
加利福尼亚州好莱坞(美国)。

(21)　APPL。编号：**15/886,432。**

(22)　提交：　　**2018 年 2 月 1 日。**

相关的美国申请数据。

(注 60)临时申请第 62/454,423 号，于 2017 年 2 月 3 日提交。

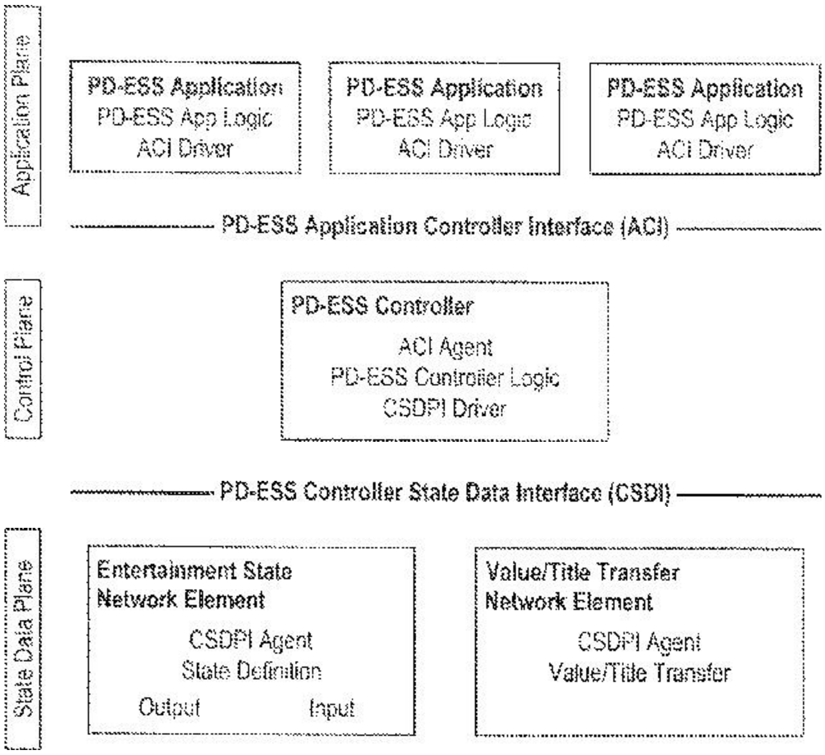
出版物分类。

(51)内部。**克莱。**
G06N 3/08(2006.01)。
G06K 9/00(2006.01)。
G06Q 20/06(2006.01)。
G07F17/32(2006.01)。

(52)美国。
CPCG06N 3/08(2013.01)；G07F ***17/329。***
(2013.01)；G06Q20/065(2013.01)；G06K
9/00221(2013.01)。

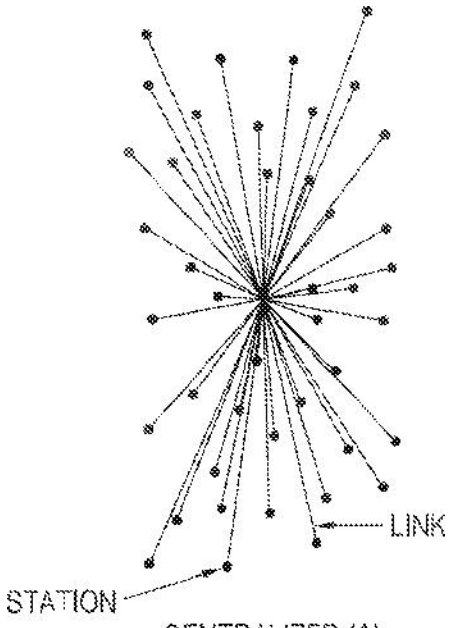
(57)摘**要。**

提供了训练人工智能系统的 FBR 系统和方法，包括使用一个或多个人类主体对刺激的反应作为人工智能系统的输入。显示器面向人类受试者，以将刺激呈现给人类受试者。检测器监视人类受试者对刺激的反应，检测器至少包括运动检测器，检测器提供输出。耦合分析系统以接收检测器的输出，分析系统提供对应于人类受试者的反应是阳性还是阴性的输出。神经网络利用分析系统的输出，当分析系统的输出为正时，生成神经网络的正加权 FBR 训练，当分析系统的输出为负时，生成神经网络的负加权 FBR 训练。



U– ‘–Upy 遂™–丕岛雀 B J。

编程 Hy Defined Gaming System(高级游戏系统)。

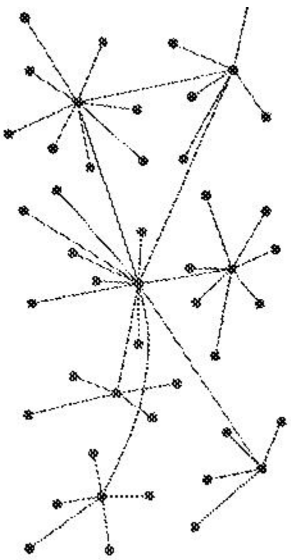


CENTRALIZED (A)

Prior Art Centralized System

F/G»1

。

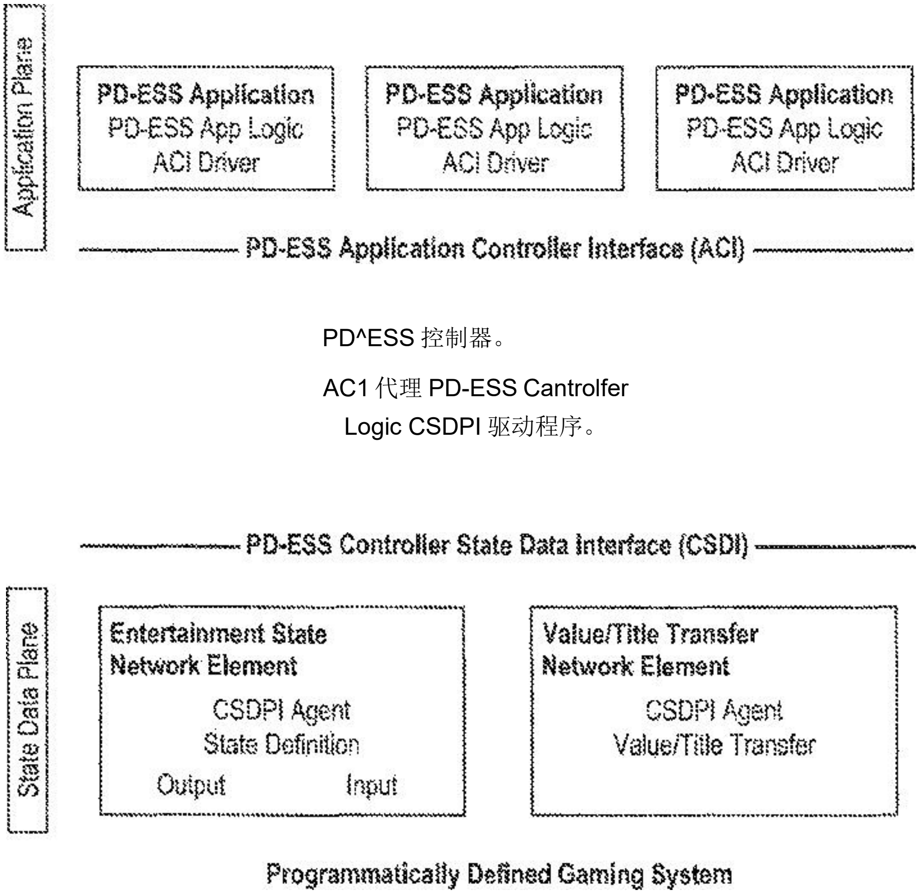


DECENTRALIZED

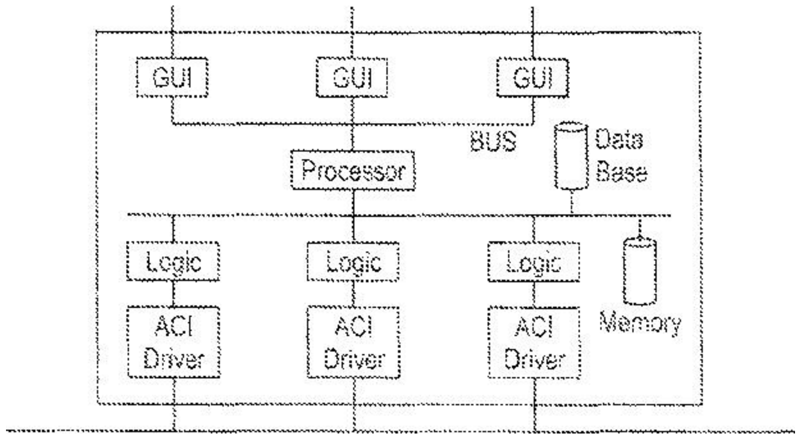
Prior Art Decentralized System

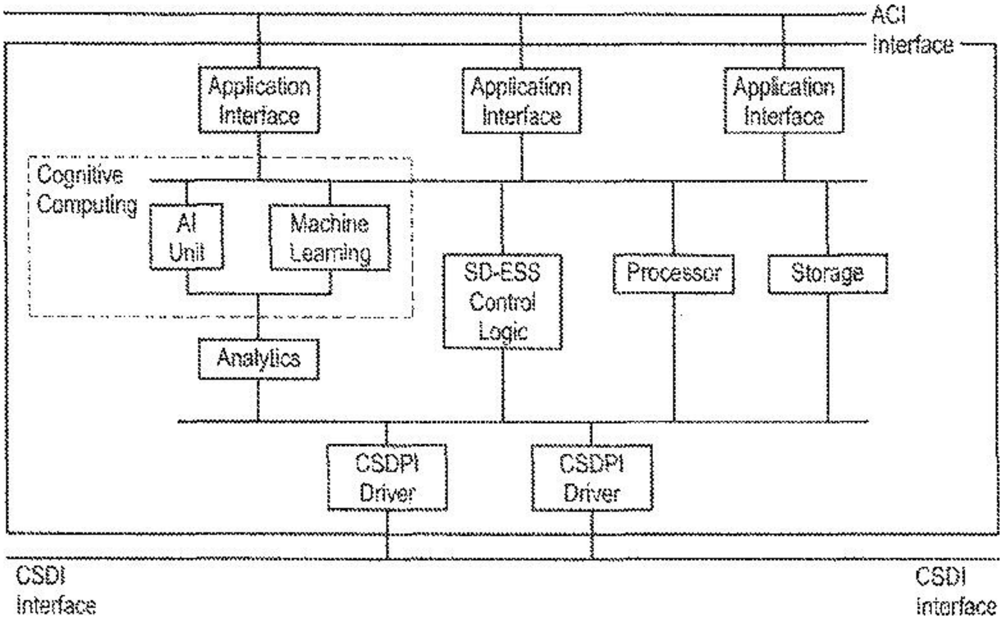
插图。2

(现有技


Application Plane
PD-ESS Application
PD-ESS App Logic
ACI Driver
PD-ESS Application
PD-ESS App Logic
ACI Driver
PD-ESS Application
PD-ESS App Logic
ACI Driver
PD-ESS Application Controller Interface (ACI)
PD^ESS 控制器。
AC1 代理 PD-ESS Cantrolfer
Logic CSDPI 驱动程序。
PD-ESS Controller State Data Interface (CSDI)
State Data Plane
Entertainment State
Network Element
CSDPI Agent
State Definition
Output
Input
Value/Title Transfer
Network Element
CSDPI Agent
Value/Title Transfer
Programmatically Defined Gaming System

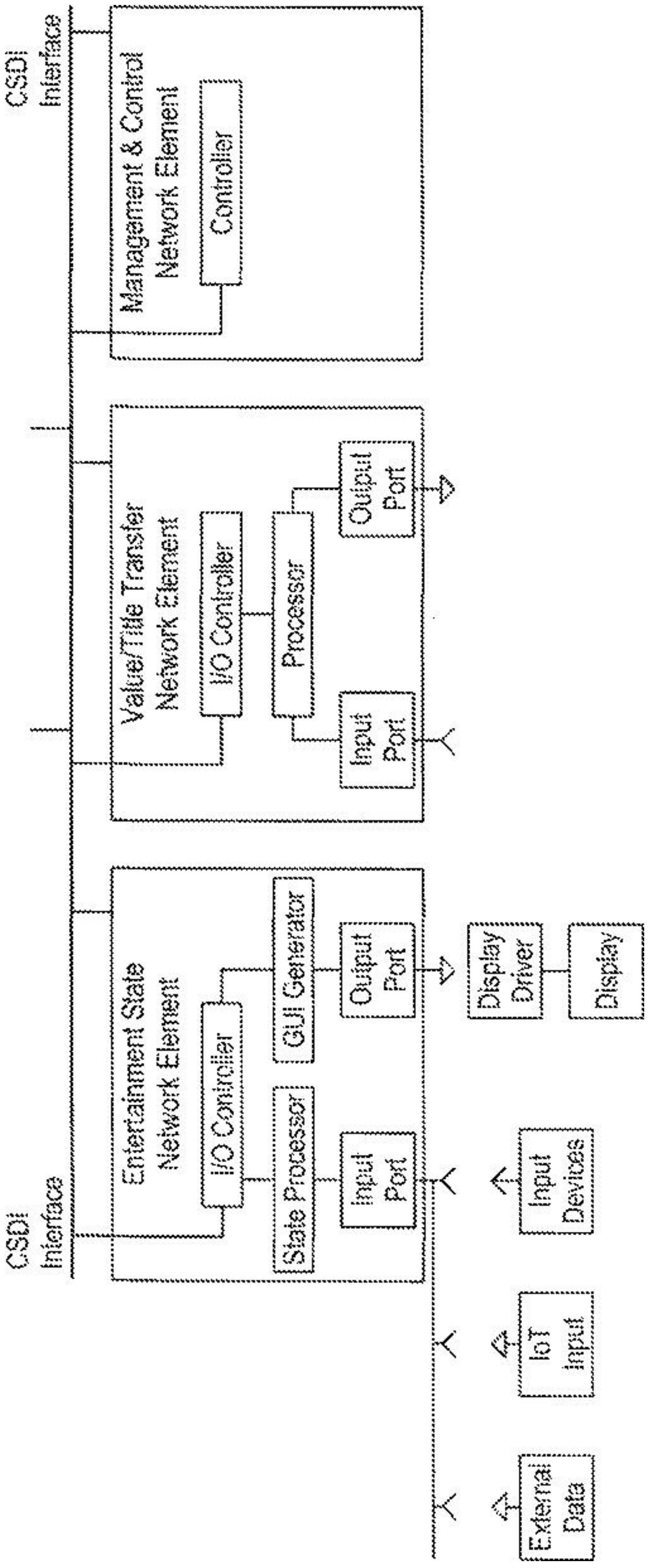
插图。3


GUI
GUI
GUI
BUS
Data
Base
Processor
Logic
Logic
Logic
Memory
ACI
Driver
ACI
Driver
ACI
Driver



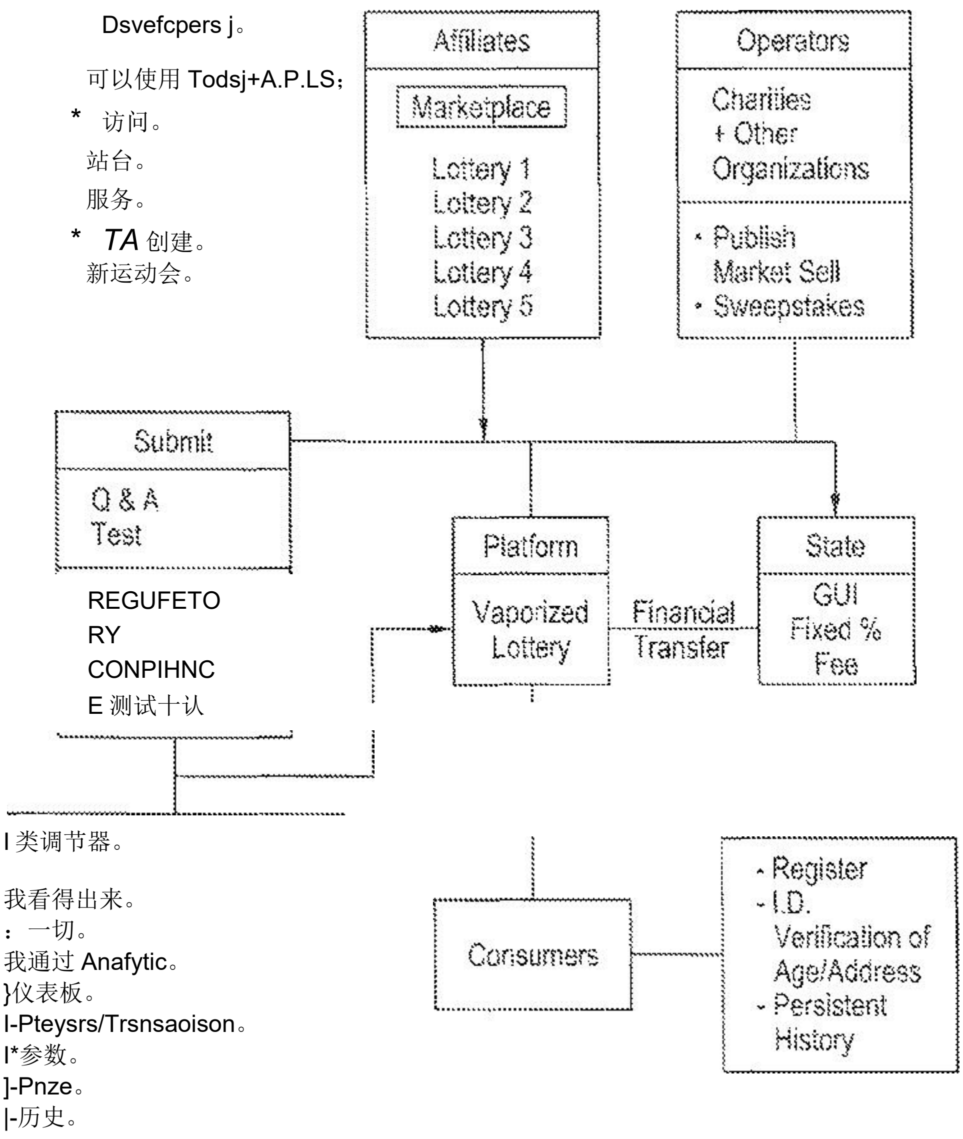
Canfml Phne Exploshn。

FIQ。5

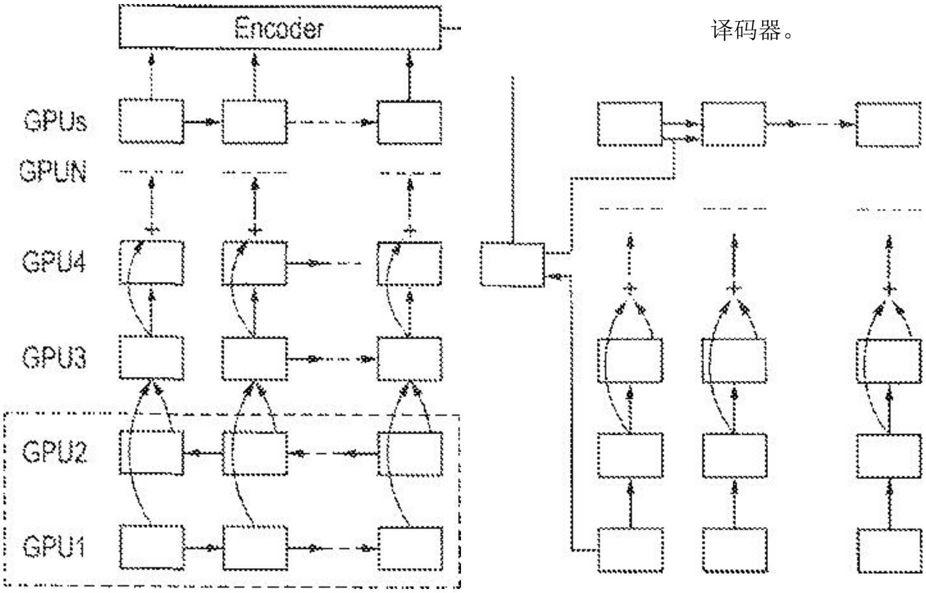


UoggoKsq®AS^JSBQ3 迄»。

9
0
.1

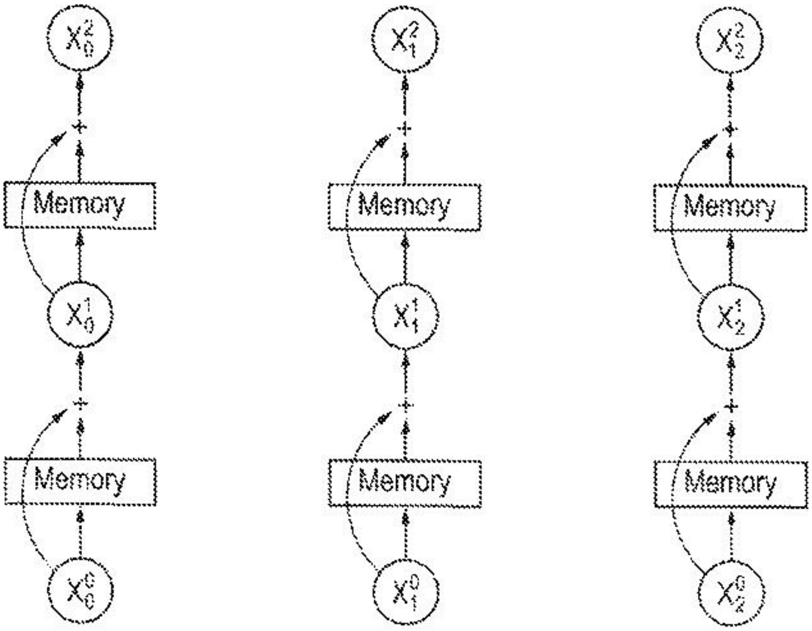


生态系统环境与生态系统集成。



Neural Network Model Architecture

FIG. 8



Neural Network

插图。9

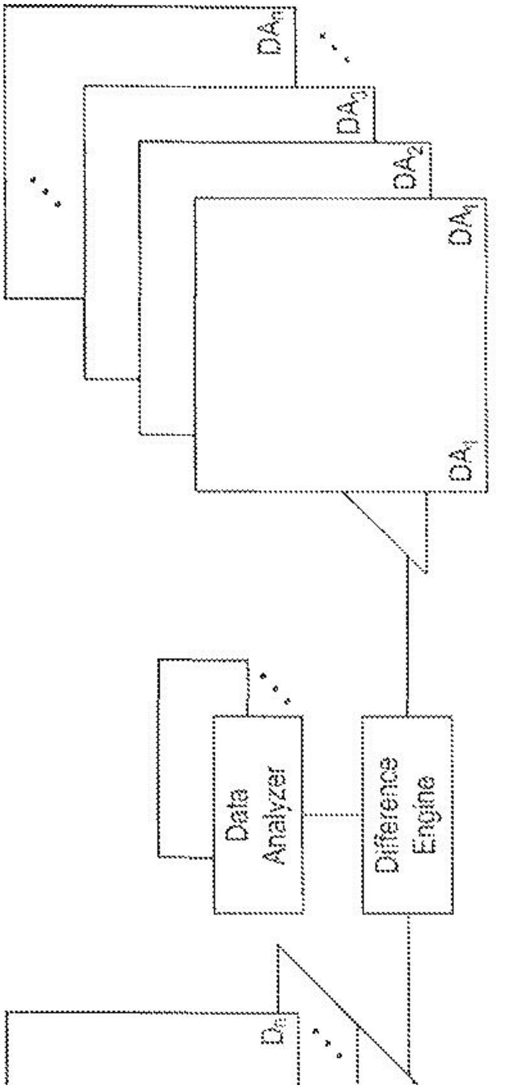
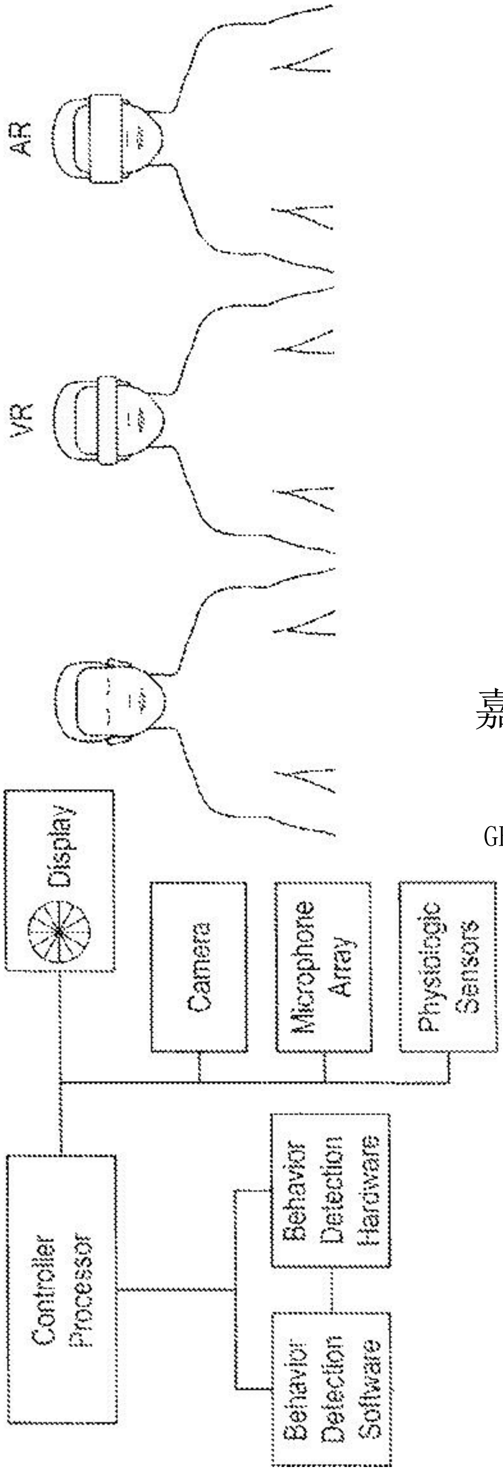


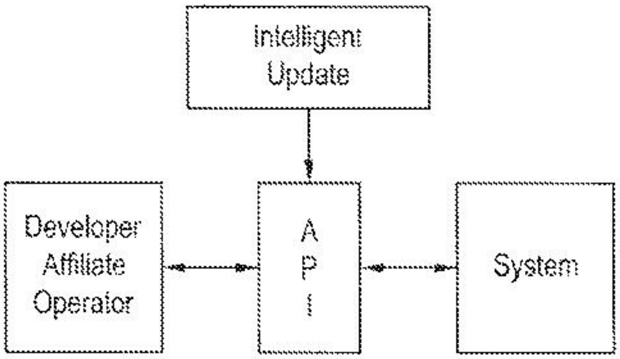
FIG. 10

专利申请公布 2018 年 8 月 30 日美国 2018 年/0247191 年度第 8 页。



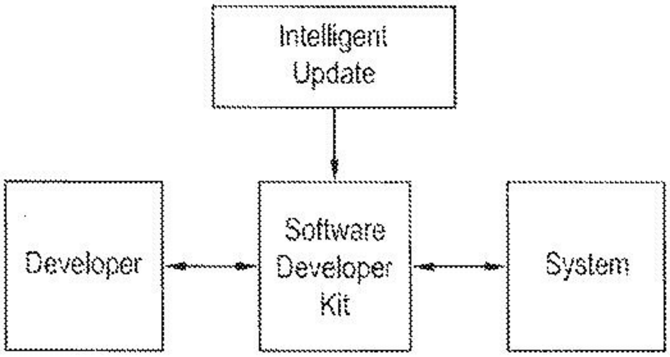
嘉 0 过。

GB>6 GE 卷睡若>
J . .
噎 2 瑟 堂噬 安 蕊
潘愁<。
Ow.B-fo。



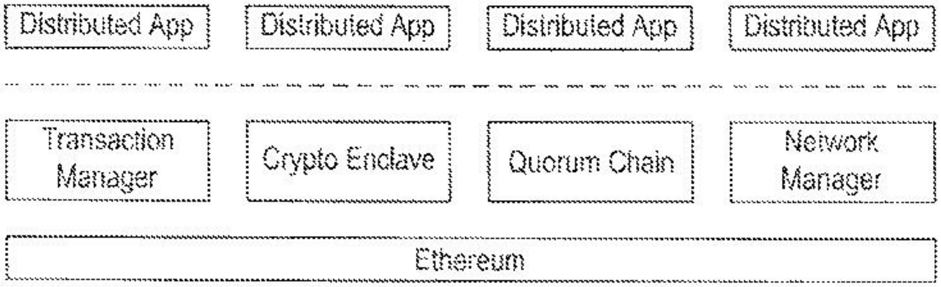
Dynamic Systems d-API

FIG. 12



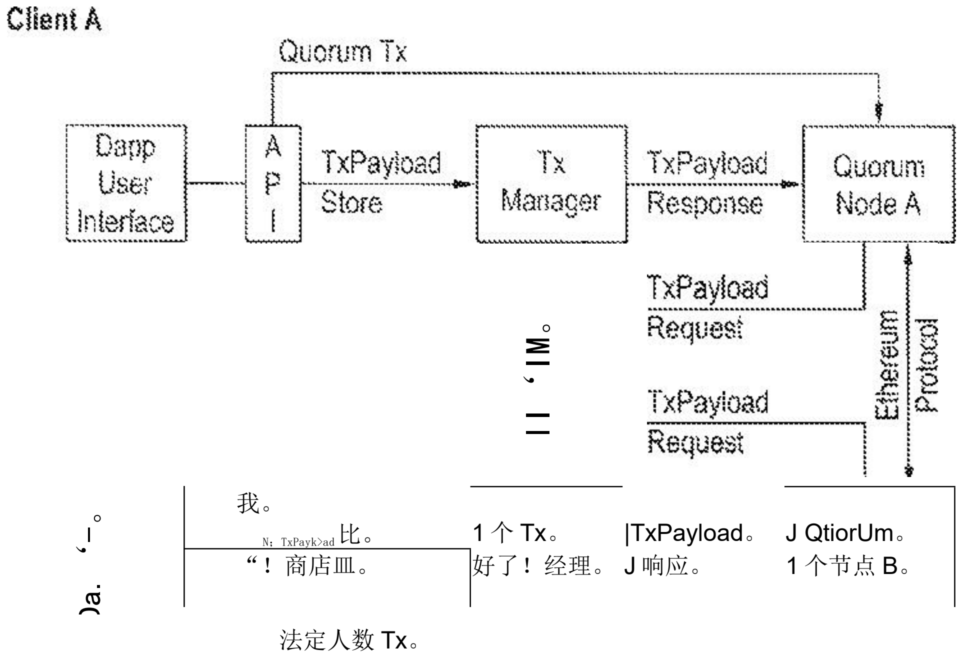
Dynamic Systems d-SDK

FIG. 13



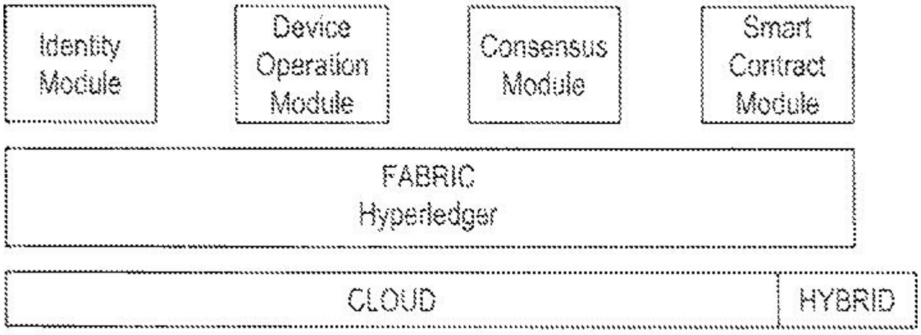
Architecture

FIG. 14

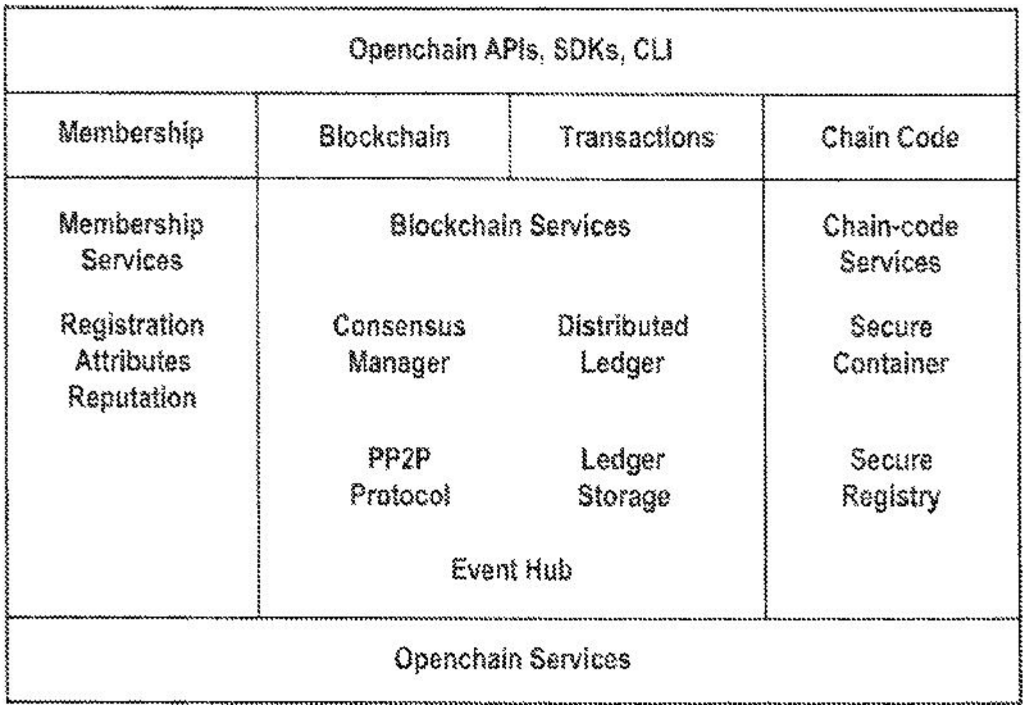


Permissioned System

FIG. 15



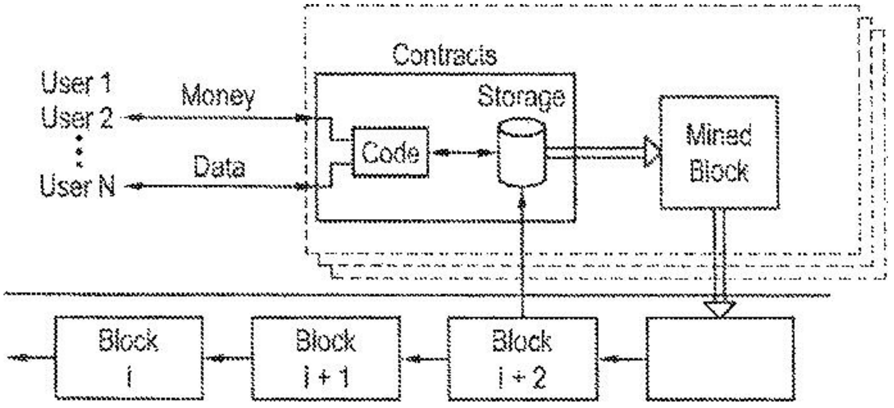
Blockchain Platform



站台。

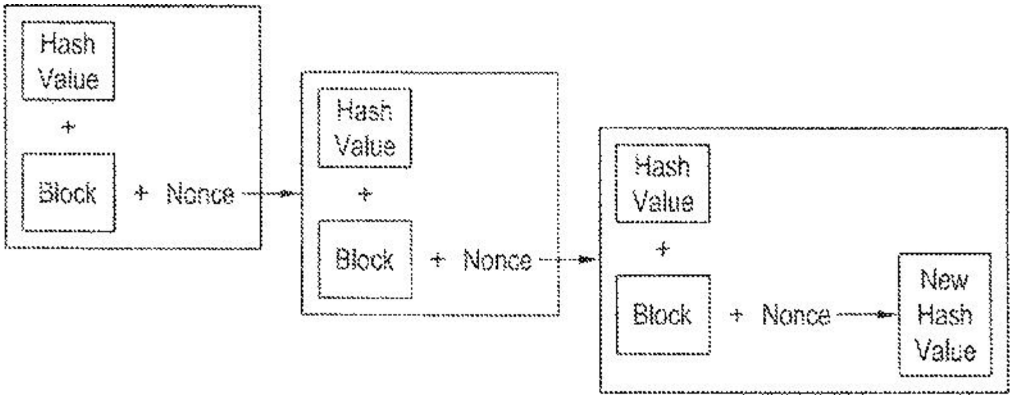
图17。

矿工。



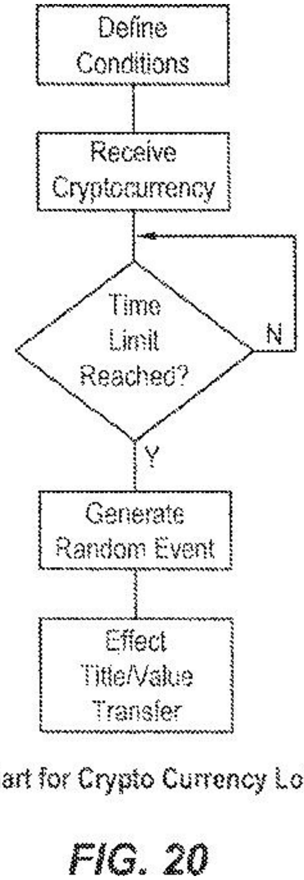
Schematic of a Decentralized Cryptocurrency System with Smart Contracts

18



顺序 Hash Vafae 创建示意图(Hash Value Pkss Stock Plus Nonee New Ha^h Vslus)。

F/G。*19*

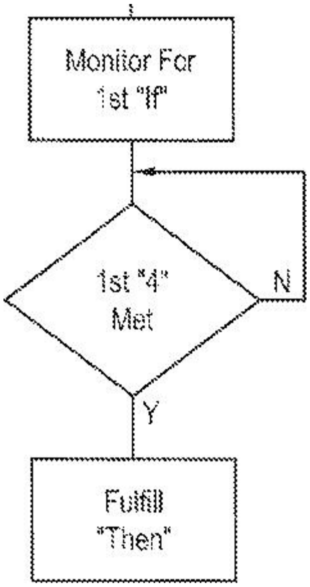


Flowchart for Crypto Currency Lottery

FIG. 20

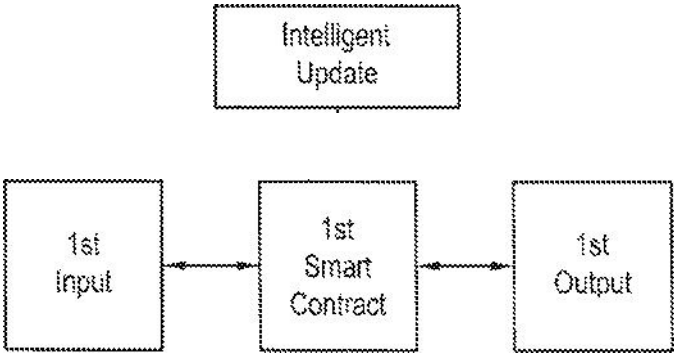
我我。

如果*[一一 w瓯竺_i。

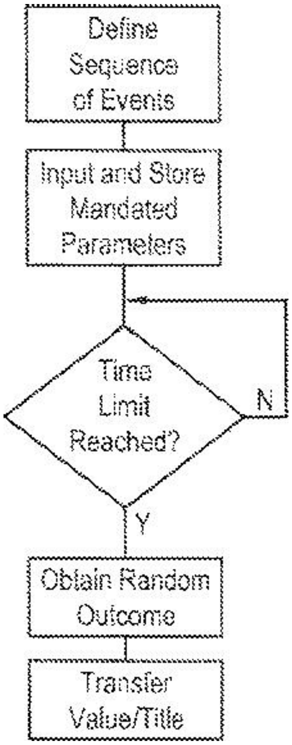


智能契约。

插图。21

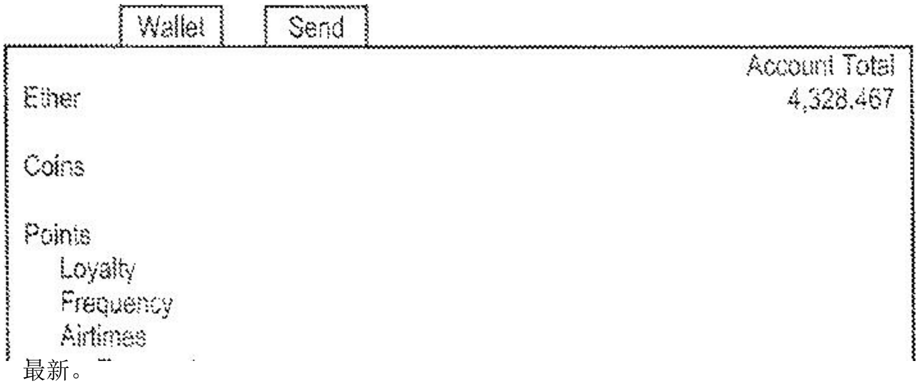


智能-智能(Smart2)合同。



Smart Contracts with Mandated and Variable Parameters

FIG. 23



Account Total
4,328,467

Ether

Coins

Points
Loyalty
Frequency
Airtimes

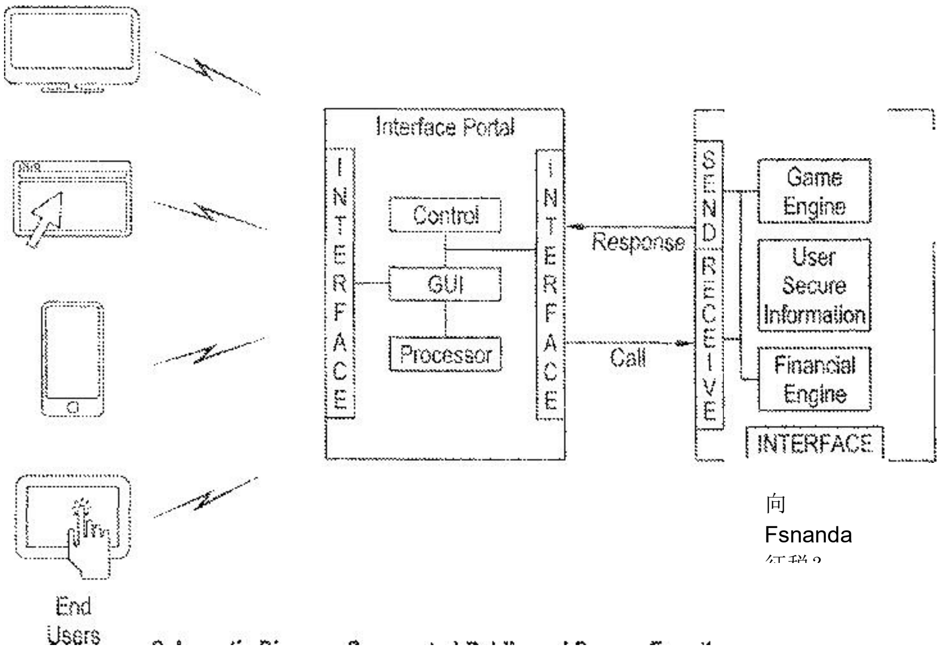
最新。

；4月12日转会 Betveen WAhls 10 公司。

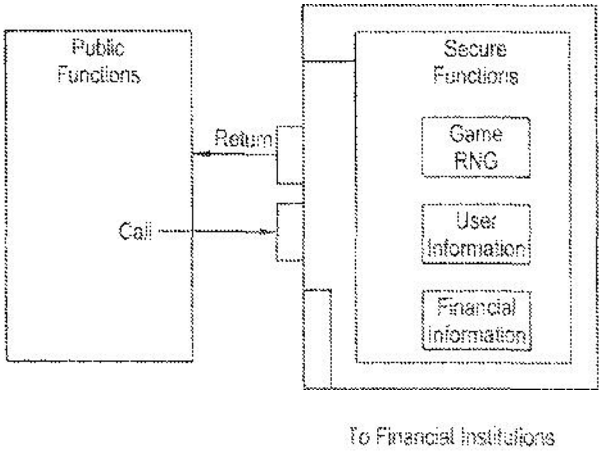
我达信 3G 购买 8，37 Cosn。

\Febajary 2 Rswsrd Po-FSH 11007 点。

插图。24

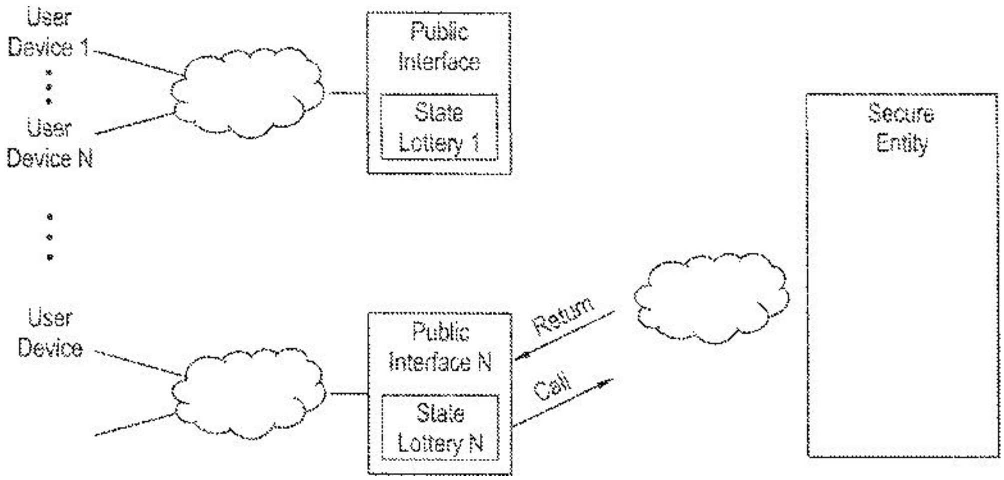


插图。25



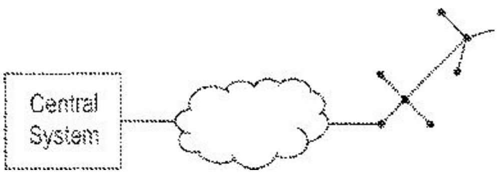
Interface of Segregated Secure and Public Functions

插图。

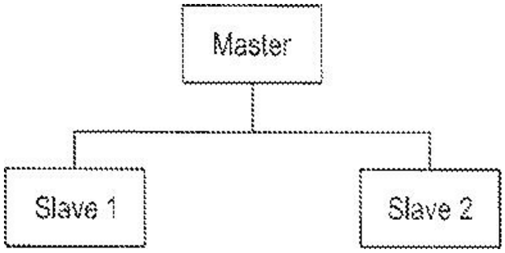


Network Implementation of Segregated Secure and Public Functions

胡。ZR。

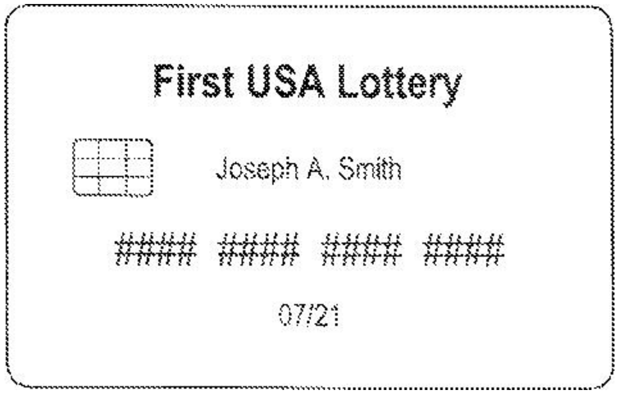


Centrslksd 击去中心化系统。



HssRarehjcal 系统。

插图。29



彩票 Lhiksd 信用卡。

插图。30

用于节目定义的娱乐状态系统、分散的加密货币系统和具有分离的安全功能和公共功能的系统的体系结构、系统和方法。

优先权申请。

[0001]本申请要求对 2017 年 2 月 3 日提交的美国临时申请 62/454,423 的优先权，该临时申请的标题为“用于程序定义的娱乐国家系统、分散式加密货币系统和具有分离的安全功能和公共功能的系统的体系结构、系统和方法”(ArchitectURe，Systems and Methods for ProgRam Defined Entertainment State System，Distributed Encryption CURrency System)。

本发明的领域。

[0002]本发明涉及用于以编程方式控制的娱乐状态系统的体系结构、系统和方法。更具体地，涉及利用认知计算进行程序控制的体系结构、系统和方法，包括但不限于人工智能和机器学习，并且可选地包括分析。提供了系统、方法和体系结构，利用可选地在对等系统中的包括区块链的分散系统来提供 FBR 游戏和娱乐操作。更具体地说，涉及在分散系统中利用诸如比特币的加密货币实现彩票、游戏或娱乐的系统和方法。

发明背景。

[0003]历史表明，为了提供社会和企业的 FBR 高效运作，许多可信系统已经发展。一般来说，这些都涉及对系统的集中控制，以确保遵守规则。在游戏领域，例子包括彩票和受监管的游戏。例如，内华达州博彩管理委员会监督该州博彩管理机构遵守法律法规的情况，并确保该行业公平和高效地运作。

[0004]考虑一下娱乐和游戏系统背景。彩票是一种“国家”功能，是一种“信任代理”。彩票要素的经典定义是奖金、机会和对价。当这些元素按更正确的时间顺序重新排序时，即首先，收到并持有对价(例如，购票)、机会(例如，确保公平和准确的随机数生成器)和奖品(即，将奖金支付给真正的获胜者)。因此，国家充当一个“信托代理人”，因为它持有对价，保证“4 次机会”的随机性，并支付奖金(所有权转让)。“信任”是建立在系统运营者和监管机构的诚信和可信度的基础上的。彩票或州监管机构往往是前执法人员。对监管机构的信任程度通常基于时间和过往记录，例如，内华达州监管系统被认为是高度值得信赖和有效的，部分是基于数十年的过往记录。此外，在监管过程中失去信任最容易造成企业损失的州最有动力提供监管。这样的系统基于对系统的集中控制。

[0005]赌场是一种四国管制的功能，是一种经过验证的“委托代理”形式。它们由国家颁发许可证，并接受国家检查。

[0006]在游戏和娱乐环境中取得了各种进步。以下内容转让给本协议的受让人，并以引用的方式并入本文中，如同在此完整阐述：游戏，以及在机会游戏和技能游戏中改进游戏的方法，美国帕特。第 6,565,084 号，游戏，以及 FBR 在机会游戏中的方法和设备，美国 PAT。第 6,488,280 号，游戏，以及 FBR 在机会游戏中的方法和设备，美国 PAT。编号 6,811,484，设备和方法 FBR Game play in a Electronic Environment，U.S.PAT。编号 8,393,946，设备、系统和方法 FBR Implementing Enhanced Gaming and Priking PaRameters in a Electronic Environment(在电子环境中实现增强型游戏和奖励参数的 FBR)，美国专利。编号 7,798,896，设备、系统和方法 FBR Implementing Enhanced Gaming and Priking PaRameters in a Electronic Environment(在电子环境中实施增强型游戏和奖励参数的 FBR)，美国专利。编号 8,241,110，方法和设备 FBR 增强彩票和游戏环境中的游戏，美国专利。编号 8,727,853，方法和设备 FBR Enhanced InteRactive Game Play in Lotting and Gaming Environment，U.S.PAT。No.8,241,100，Method and System FBR Electronics InteRaction in a Multi-Player Gaming System(多玩家游戏系统中的 FBR 电子交互)。美国帕特。8,535,134 号。通常，它们由一套工具组成，以使系统更具吸引力，并优化结果。

[0007]大型系统中的一个令人烦恼的问题是系统不兼容。各种组件通常来自不同的供应商。通常缺乏互操作性和不兼容性。游戏生态系统中的各种系统需要互操作，包括但不限于：游戏运营、营销、CRM(客户关系管理)、忠诚度计划、辅助积分或积分、系统分析和优化以及账户和审计功能。

[0008]软件定义系统是在更高级别的软件控制下互操作的模块集合。它们通过抽象较低级别的功能来管理网络服务。一般来说，存在应用平面、控制平面和数据平面。示例包括具有控制平面的软件定义网络，该控制平面提供对由相对较不智能的交换机、路由器、存储器组成的数据平面的智能控制。另一个例子是软件定义的无线电。控制平面监视和监督数据平面中频段的使用。

[0009]另一个组件是使用静态接口和工具。例如，API 或应用编程接口通常包括静态接口。它们定义了信息请求的格式 FBR。“如果你以特定的方式询问 FBR X，我们会提供 Y‘。一般情况下，除了通过 API，请求者不会提供对系统的访问。还有一个系统是 SDK，即软件开发工具包(Software Development Kit)。它们可能是静态的。提供了实现预期结果的工具。GDK 或游戏开发工具包也可以是静态的，并提供 FBR 游戏开发工具。

[0010]娱乐或游戏的设计通常由度量驱动的设计驱动。这通常涉及 A/B 测试，比较多个系统之间的结果或优惠度。此外，他们经常监测多变量反应系统。

[0011]彩票和乐透风格游戏的一个方面是它们往往是静态的。在最极端的例子中，它们是。

字面上印在纸板上。更广泛地说，一旦选择了彩票游戏的格式，例如 49 种格式中的 6 种，就很难改变。公众对变化的看法是，这个游戏对玩家变得不那么有利了。

[0012]赌博问题一直困扰着博彩业。这对社会来说是一个重大问题。虽然用户可以寻求帮助(例如，1-800-Gamling)，但通常会有拒绝和不愿意寻求帮助的情况。已经进行了各种尝试来限制滥用，例如在一些在线游戏中使用速率限制。

[0013]在从实体领域向在线和网络领域转移的过程中，身份问题激增。问题包括：你是你声称的那个人吗？用户的身份会被泄露吗？

[0014]认知智能和适应性智能取得了重大进展。例如，IBM Watson 在 2011 年与高技能选手举行的“危险边缘”(Jeopardy)比赛中获胜。深度学习和模式识别已经出现。目前的趋势包括大数据、模式识别和机器学习。

[0015]在 2D 和 3D 空间中的目标检测方面也取得了最新进展。大规模视觉识别挑战赛(LSVRC)中的一项挑战在 ImageNet 2016 中提供了 FBR 对象检测。ImageNet 的自动标签错误率降至不到 3%，而人工操作的错误率约为 5%。

[0016]在基于机器的游戏性能方面也取得了重大进展。2015 年，Google Deep Mind 使用人工智能强化学习系统学习如何玩 49 款雅达利游戏。2016 年，谷歌的 AlphaGo 系统以 4：1 击败了世界上最伟大的围棋选手之一。2017 年，卡内基梅隆大学(Carnegie Mellon University)的 LiBRatus 项目以统计意义上的方式击败了顶级人类选手。

[0017]在基于云的系统方面取得了进一步的进展。功能已经从本地服务器和存储迁移到远程“云”存储。这些系统提供了 FBR 轻松的可扩展性。基于云的系统可以同时运行多个 4 个实例。他们还可以结合软件即服务，包括人工智能(“Al”)。

[0018]物联网(IoT)利用能够向远程位置发送数据和接收命令数据的设备。各种语音控制设备使用人工智能或机器学习(ML)，例如 AmAzon Alexa、Google Dot。**[0019]图 1.**。**1** 示出了示例性的现有技术集中系统。插图。**2** 示出了示例性的现有技术分布式系统。

[0020]在可信分布式系统中取得了进步，例如在使用基于区块链的系统方面。区块链技术的最初披露归功于中本聪(Satoshi Nakamoto)在 2008 年 10 月发表的一篇论文。该系统提供 FBR 自动信任或系统信任。区块链范式为 FBR 提供了一个利用分散共识的分散系统。这可以在没有中介的情况下以点对点的方式完成。该系统可以被视为在可编程分布式网络上运行软件的节点网络。它有时被称为具有共享状态事务单例机器、基于事务的状态机、消息传递框架、可信对象消息传递计算框架和可信计算。

[0021]区块链和密码学的结合建立了分散共识。权威和信任。是由分散的虚拟网络提供的。共识逻辑通常与应用程序分开。它可以包括分散架构的第一层。

[0022]区块链使用分布式分类帐。“块”由一组新的已接受事务组成。一批交易在一块中被释放，以由参与计算机的网络进行验证。公共区块上连续的、顺序的交易记录创建了唯一的“链”或区块链。此块将发布到所有其他节点。该出版物定期发布，例如每 10 分钟发布一次。

[0023]EtheriUm 是一个开源的 FBR 智能合约平台。就目前的运营而言，EtheriUm 是一个运行智能合同的去中心化平台：应用程序完全按照程序运行，没有任何停机、审查、欺诈或第三方干扰的可能性。这些应用程序运行在定制的区块链上，这是一种极其强大的共享全球基础设施，可以移动价值并代表财产的所有权。这允许开发商根据长期的指示(如遗嘱或期货合约)创建市场、存储债务或承诺记录、转移资金，而不存在交易对手风险。EtheriUm 还表示，其目标是创建一种可交易的数字令牌，可以用作货币、资产的表示、虚拟份额、成员资格证明或任何东西。这些代币使用标准的硬币 API，因此合同将自动与任何钱包、也使用此标准的其他合同或交易所兼容。流通中的令牌总量可以设置为简单的固定量，也可以根据任何编程规则集进行浮动。总而言之，EtheriUm 表示，它可以建立一个固定供应的可交易令牌，一个可以发行货币的中央银行，以及一种基于谜题的加密货币。

[0024]当前的系统有许多缺点。他们改变和创新的速度很慢。它们通常涉及不能互操作的专有系统。这往往存在政府和/或体制上的偏见。可能会有一个繁琐的监管环境。最后，交易成本往往很高。

[0025]因此，需要在不一致的、通常是专有的系统之间进行 FBR 互操作性。有必要在更全球化的基础上限制 FBR 赌博，包括地理模拟和全球使用率监测 FBR 问题赌博。有必要对 FBR 问题进行赌博检测和补救。因此，需要对分布式系统进行 FBR 改进。

发明内容。

[0026]提供了 FBR 训练人工智能系统的系统和方法，包括使用一个或多个人类主体对刺激的反应作为人工智能系统的输入。一个或多个显示器朝向人类受试者以向人类受试者呈现刺激。一个或多个检测器用于监视人类受试者对刺激的反应，所述检测器至少包括运动检测器，所述检测器提供输出。耦合分析系统以接收检测器的输出，该分析系统提供对应于人类受试者的反应是阳性还是阴性的输出。神经网络利用分析系统的输出，在分析系统的输出为正时提供神经网络的正加权 FBR 训练，在分析系统的输出为负时提供神经网络的负加权 FBR 训练。

附图的简要说明。

[0027]图 2.。1 是现有技术集中式系统的示意图。

[0028]图 3.。2 是现有技术集中系统的示意图。

[0029]图 3.。3 是显示应用平面、控制平面和状态数据平面的程序定义娱乐状态系统(PD-ESS)的系统级框图。

[0030]图 3.。4 是 PD-ESS 的应用状态平面层的系统级框图展开)。

[0031]图 3.。5 是 PD-ESS 控制平面层的系统级框图爆炸)。

[0032]图 3.。6 是 PD-ESS 的状态数据平面层的系统级框图爆炸)。

[0033]图 3.。7 是生态系统的图解视图，包括接口和互连。

[0034]图 3.。8 是包括图形处理单元(GPU)的神经网络模型体系结构的系统级框图。

[0035]图 3.。9 是神经网络模型体系结构的系统级框图。

[0036]图 3.。10 是包括差异引擎和数据分析器的多个数据集的系统级图。

[0037]图 3.。11 是响应系统显示和检测系统，用于生成训练人工智能(AI)和机器学习(ML)系统的输入。

[0038]图 3.。12 是动态系统应用编程接口(D-API)的系统级图。

[0039]图 3.。13 是动态软件开发工具包(d-SDK)的系统级图。

[0040]图 4.。14 是包括区块链和以太网的分布式系统的系统架构层级图。

[0041]图 4.。15 是允许的区块链系统的系统架构层级图。

[0042]图 4.。16 是区块链平台的系统架构层级图。

[0043]图 3.。17 是包含开链服务的区块链平台的系统架构层级图。

[0044]图 3.。18 是具有智能合约的去中心化加密货币系统的系统架构层级图。

[0045]图 3.。19 是具有顺序散列值创建的分散系统的系统体系结构层级图。

[0046]图 4.。20 是加密货币彩票的流程图。

[0047]图 3.。21 是智能合约的流程图。**[0048]图 3.。22** 是智能-智能(Smart2)合同的流程图。

[0049]图 3.。23 是具有强制和可变参数的智能合同的流程图。

[0050]图 3.。24 是加密货币钱包的图形用户界面(GUI)。

[0051]图 3.。25 是具有分离的公共和安全功能的系统的系统体系结构级示意图。

[0052]图 3.。26 是分离的公共和安全功能的接口的系统体系结构级别。

[0053]图 3.。27 是具有分离的公共和安全功能的系统的网络实现的系统体系结构级别。

[0054]图 3.。28 是集中式和分散式相结合的系统架构层。

[0055]图 3.。29 是分层系统的系统架构级别。

[0056]图 3.。30 是彩票关联信用卡的平面图。

本发明的详细描述。

[0057]用于节目定义的娱乐状态系统的体系结构、系统和方法。

[0058]下面的描述主要结合图 3。**3**、**4**、**5** 和 **6**，但也可适用于其他数字。提供了一种体系结构，该体系结构是节目定义的娱乐状态系统。这优选地用于将控制整体体验的系统与定义状态的底层系统分离。第一平面即应用平面提供接口，主要是 FBR 系统侧用户，例如事件、竞赛、彩票的组织者、开发者。第二个平面，控制平面，提供 FBR 智能控制，特别是认知计算，包括人工智能和/或机器学习，包括系统随着时间学习的人工智能。这优选地在模块之上提供智能控制层。第三平面，即状态数据平面，为 FBR 娱乐 4 状态模块提供各种机制，优选地包括“核心环路”、元状态，并提供接口 FBR 终端用户以及输入和输出。

[0059]图3.。3提供了框图程序定义的娱乐状态系统(PD-ESS)。插图。4 是 PD-ESS 应用平面层的爆炸式增长，包括应用层 GUI(面向开发人员、分支机构和慈善机构)。插图。**5** 提供爆炸 PD-ESS 控制器平面层。插图。**6** 提供爆炸 PD-ESS 状态数据平面层。还包括娱乐状态网元层的爆炸性增长、用户界面 GUI、价值/所有权转移网元的爆炸性增长以及其他功能块的爆炸性增长。

[0060]首先转到应用平面层，程序用于向 PD-ESS 控制器传达要求和期望的行为。它通过 PD-ESS 应用控制器接口(ACI)提供 PD-ESS 应用和 PD-ESS 控制器之间的通信。可选地提供应用程序逻辑和驱动程序。应用层可以接收状态数据平面动作的抽象视图。PD-ESS 应用程序可以与更高级别的抽象控制接口。该系统包括一个接口，即 PD-ESS 应用控制器接口(ACI)。优选地，该管理和管理提供以下内容：(1)到/从应用平面，它提供合同和 SLA，(2)到/从控制平面配置策略，监控性能，以及(3)到/从数据平面元素设置。

[0061]第二转到控制平面层，PD-ESS 控制器在理想的逻辑上是集中式实体，优选地用于将 PD-ESS 应用的要求转换到状态数据平面层，并向应用层提供状态数据平面中的动作(例如，事件信息和统计信息)。控制平面可以从数据平面向应用平面提供统计数据、事件和状态。控制平面优选地在数据平面中的低级控制处实施行为，提供能力发现，并监视统计数据和故障。控制平面有利地包括认知计算，诸如人工智能(Al)和机器学习(ML)，下面将更详细地描述。

[0062]控制平面可以可选地包括分析，包括但不限于模式识别。可以对群体(最好是相关群体)或子集执行分析。优选地，该子集具有与目标用户相似的特征。数据可以根据子集入库。可以分析原始数据的范围。可以包括预测建模。可以在控制平面级别实施负责任的游戏控制，特别是在存在使用率限制和全局限制的情况下。

[0063]第三，转向状态数据平面层，其优选地包括主要子组件和功能网元。可选地，功能网元包括以下部分或全部。1.。娱乐状态网元，2.。价值/所有权转让网元，3.。游戏库，如赌场，VET，电子游戏，锦标赛，有奖游乐设施(AWP)，游戏机制，核心循环，技能，揭秘技能，第二次机会，社交，游戏化，奖品，vGLEP 和奖牌，4.。系统、市场营销、促销、CRM、运营、物流、互动、移动/应用程序和响应性设计，5.。站台，6.。频道，7。彩票，包括零售和中央系统，8。忠诚度，9.。负责任的游戏控制，可选地包括使用率限制和全局限制(也可以在控制平面层进行)。10.。体育，包括现实世界、梦幻和电子竞技，11 分。Other Live Data Entertainment，12。网络，包括网络通信和网络服务以及 13。管理，包括记录、玩家账户管理、报告、合规性(包括法规遵从性)、安全(包括网络安全、欺诈和风险管理，最好包括审计和支付)。

[0064]娱乐状态网元提供与系统用户的接口 FBR 交互。输入从用户选择接收信息。传感器可以是各种形式，包括声音传感器、运动传感器，无论是 2-D 还是 3-D，例如包括微软 Kinect 系统。“内部数据”主要由与游戏操作相关的数据组成。“要与主数据源组合的 ExtemaF 数据源。这些可能包括 1 个。位置，2。当前活动，如驾驶(由车辆提供，由跟踪电话提供)或锻炼(由 FitBit 或类似工具提供)，3.。经济状况，4.。天气，5。最近的事件/新闻，例如，最近的一次大型强力球胜利，6.。营销信息，7.电子邮件扫描，例如，谷歌扫描 Gmail FBR 内容，8.。社交媒体，以及 9.物联网(LOT)。物联网(LOT)提供了各种形式的互联设备，如数据传感器。传感器产生数据输入“刺激”到系统。通过利用任何形式的输入，该系统能够提供 FBR 大规模并行性。对系统的所有数据“刺激”允许系统对所有数据刺激进行自适应和反应。

[0065]输出为用户提供刺激。表单可能包括：1.图像，例如在显示器上，或通过 GUI 或 VR 系统、AR 系统，2.。具有远程计算能力的瘦客户机显示器，3.。投影和全息图，4.声音，5.触觉刺激，6.嗅觉刺激，或 7.神经或其他直接电刺激。

[0066]价值/所有权转移网元用于接收和转移价值(货币、硬币和其他有价值的物品)。价值可以指可替代的流动资产或其他价值储存。所有权一般指不动产、动产或虚拟财产的所有权。下面详细讨论了区块链、无信任和加密货币系统。

[0067]人工智能(AI)广泛地说是计算机科学中处理智能行为自动化分支。它们是系统，其目标是使用机器来模拟和模拟人类的智能和相应的行为。这可以采取多种形式，包括符号或符号操作 Al。它可以解决分析抽象符号和/或人类可读符号的问题。它可以在数据或其他信息或刺激之间形成抽象连接。它可能会形成合乎逻辑的结论。人工智能是机器、程序或软件所展示的智能。它被定义为智能 Agent 的研究和设计，其中智能 Agent 是一个感知环境并采取行动最大化成功机会的系统。还有一些人将其定义为制造智能机器的科学和工程。

[0068]人工智能通常涉及到神经网络的使用。在各种实施例中，使用神经网络节点的多层堆栈。最低层由颗粒状元素组成。作为游戏应用中的示例，按照更高级别理解的顺序，级别将从单个动作的实例(粒度)、核心循环检测、会话播放、到多会话播放进行。可选地，解析引擎用于将较大的集合(例如数据集或图像)分解或细分为更离散或更细粒度的元素。

[0069]Al 可以具有各种属性。它可能有演绎、推理和问题解决。它可能包括知识表示或学习。系统可以执行自然语言处理(通信)。还有一些人执行感知、运动检测和信息处理。在更高的抽象层次上，它可能会产生社交智力、创造力和一般智力。采用了多种方法，包括控制论和脑模拟、符号、次符号和统计学，以及整合这些方法。

[0070]可以单独或组合使用各种工具。它们包括搜索和优化、逻辑学、概率方法、FBR 不确定性推理、分类器和统计学习方法、神经网络、深度前馈神经网络、深度递归神经网络、深度学习、控制理论和语言。

[0071]A1 在其体系结构中有利地利用并行处理，甚至大规模并行处理。图形处理单元(GPU)提供 FBR 并行处理。当前版本的 GPU 可从各种来源获得，例如 NVIDIA、Nervana Systems。

[0072]机器学习被定义为从经验中构建知识的系统。机器学习用于发现模式和规律。

[0073]深度学习使用神经智能。它易于扩展，通常涉及更多层或神经网络(NN)。神经网络可以有多种形式，包括：有效神经网络、矢量化神经网络、矢量化 Logistic 回归、矢量化 Logistic 回归梯度输出、二分类、Logistic 回归、Logistic 回归代价函数、梯度下降、导数、计算图和 Logistic 回归梯度下降。

[0074]深度神经网络(DNN)通常涉及超参数调整。通常，它们利用正则化和最优化。有时它们被称为深度信念网络(DBN)。

[0075]其他形式的神经网络包括卷积神经网络(CNN)或递归神经网络(RNN)。可用系统的示例包括：

LSTM、Adam、Caffe、Dropout、Batch Norm、Xavier/He、Python、Scikit-Leam 和 TensorFlow。

[0076]A1 可以对各种形式的数据集进行操作。数据集可以包括图像，无论是视频图像、2D 数据和/或 3D 数据。可以分析顺序数据。示例包括但不限于自然语言、音频、自动驾驶决策、游戏状态和游戏决策。

[0077]各种工业应用有利地受益于铝的应用。它们包括成像和目标检测，用于识别、分类、挖掘和可选地提供情感分析。其他应用包括自动驾驶。然而，其他应用包括机器人和机器人技术。在医疗保健领域，功能包括成像分析、诊断和游戏化。可以增强各种形式的顺序数据分析，例如语音识别和自然语言处理。音乐应用包括识别和合成。在游戏领域内，应用包括游戏状态序列检测、分析、编队、组合优化和游戏优化。聊天机器人和机器翻译有利地使用了这些系统。

[0078]图 3.。7 显示了娱乐或游戏生态系统内的组成功能块。附属公司的作用是获得客户。附属公司收取佣金，例如根据获得的用户数量或收入的百分比(%)。可选的是，还有一个指向信用卡功能的链接(将在下面讨论)。

[0079]接下来是计划举办彩票、游戏或其他娱乐活动的慈善机构和其他组织。他们提供客户获取服务。他们是活动(游戏、彩票或娱乐)的接受者。他们还收取费用。

[0080]接下来是开发人员，他们提供游戏设计。作为游戏设计的回报，他们获得了多司法管辖区的使用和付费 FBR 的使用。可以提供增强的应用或应用商店，其中可以查看、选择和下载游戏设计。

[0081]接下来，消费者提供注册和标识信息。注册数据可以可选地包括身份、年龄、地址和验证。(可选)数据充足，系统可以通过可选的身份验证级别遵守了解您的客户(KYC)规则。这将存储为永久历史记录。客户获得了玩、赢和接受娱乐的机会。

[0082]接下来是监管机构或信任验证代理。他们提供测试、审批、FBR 游戏公平、整体审批，确保合规和安全。系统授予监管者或信任验证代理对每笔交易(分析仪表板)、玩家帐户、参数、奖金金额和支付以及完整历史记录的访问权限。监管机构或信托验证代理机构获得补偿，无论是费用还是交易金额的一定比例。**[0083]接**下来，彩票充当信托代理，并收取交易额的一定比例。可选地，当彩票的历史功能由生态系统内的另一实体执行时，这些功能可以从系统中消除或蒸发。

[0084]无花果。8 和 **9** 涉及 FBR 训练神经网络的学习过程。通过提供重复的输入刺激，然后训练神经网络以提供正确的输出，可以教导系统形成正确的。基于一个或多个输入激励的关联输出。在将输入转换为期望输出时，训练可以包括监督学习，例如当目标值和参数被监督时。或者，训练可以是非监督学习，其中系统试图识别输入中具有可识别结构并且可以再现的模式。或者，系统可以使用强化学习，它独立工作(类似于无监督学习)，但根据成功或失败来奖励或惩罚。优选地，强化学习涉及增量改变。在各种训练技术中，可以使用扰动，其中一个或多个输入参数通常以例如小于输入值的 10%、更优选地小于 5%和更优选地小于 3%的扰动量变化，以便监视扰动对输出的影响。在各种训练技术中，可以使用扰动，其中一个或多个输入参数通常以小于输入值的 10%、更优选地小于 5%和更优选地小于 3%的扰动量变化，以便监视扰动对输出的影响。

[0085]超参数和参数可以在 AI 或机器学习系统中使用。模型参数是根据数据自动估计的。可以根据数据估计模型内部的配置变量。这可能是模型在进行预测时所要求的。值定义了模型的技能。它们可以通过数据进行估计或学习。

[0086]超级参数是手动设置的，并在流程中用于帮助估计参数。使用模型外部的配置变量。一般来说，它不能从数据中估计出来。它们经常用于估计模型参数的过程中。它们通常由系统用户指定。通常可以使用试探法设置超参数。它们经常被调整为 FBR，这是一个给定的预测建模问题。超级分类帐可以用作超级分类帐编写器或超级分类帐结构。

[0087]可以在各种类型的硬件上执行人工智能或机器学习。有利的是，支持并行处理的系统可以提供 FBR 计算速度和效率。NVIDIA 和 AMD 提供图形处理单元(GPU)等并行处理单元。麒麟 970、Apple All 和高通 ZEROTH 处理器均配备神经处理单元(NPU)。人工智能和机器学习处理也可以作为云人工智能或机器学习系统提供，如 Google 和 AmAzon Web Services 提供的。**[0088]图 3.。10** 描述了域转换和差异引擎。一个有利的域变换涉及时域到频域(时间序列到频域)。傅立叶级数就是一个例子，它通常用于重复信号，例如振荡系统。傅立叶变换通常用于非重复信号，例如瞬变信号。可以使用诸如快速傅立叶变换(FFT)之类的增强计算技术来提高 FBR 效率和计算速度。另一种域变换是拉普拉斯变换，通常用于电子电路和控制系统。另一种是 Z 变换，通常用于离散时间信号。可以有利地使用数字信号处理器(DSP)。谱密度估计可能包括小波分析、图像分析、数据压缩和多变量分析。有利地使用相关数据集。

[0089]可以使用区分引擎来识别两组或更多组数据之间的区别。该差别可以是基于时间的，例如其中一个数据集与时间 0 有关，而另一组与时间 1、时间 2、时**间** 3、…、时间 **N** 有关。可以计算图像中的差别。

[0090]图 3.。11 示出了一个系统，在该系统中，可以监视、捕获和分析受试者的反应，然后将其用作 A1 的输入。在各种努力中，例如在游戏或娱乐设计和创作中，可以监视、分析和使用目标受众的反应来训练人工智能或机器学习系统。受试者对娱乐/游戏刺激的反应用来测量受试者所经历的‘乐趣’，然后该测量(‘FIM’)被用作 A1 或 ML 系统的训练输入。该系统可以检测个体主体行为。或者，该系统可以监视群体行为，用于检测“有趣”的体验，但也可以测量群体或人群的属性，例如兴奋、参与度或基于群体的行为。

[0091]提供显示器作为对一个或多个对象的刺激。可以使用平板显示器或监视器。可选地，可以利用个人观看设备，诸如单独的屏幕、虚拟现实耳机、增强现实设备、平视显示器、投影设备或成像技术。

[0092]利用各种检测器来监视一个或多个受试者的反应。运动检测利用运动跟踪硬件和软件。一台照相机拍摄被摄体的图像。各种摄像头包括微软 Kinect、2D 传感器和摄像头以及 3D 传感器和摄像头。度量检测器可以分析身体部位的位置，例如肢体、关节或面部特征。它可以测量速度、运动、位置或运动的更高级别的导数，如变化率。面部探测器监控 FBR 面部识别。可以检测面部属性，例如正面属性(例如，微笑)或负面属性(例如，皱眉)。可以确定身体位置检测。声音检测可以用麦克风或麦克风阵列来执行。它可以检测声音的属性，例如正面属性(例如，欢呼声)和负面属性(例如，咒骂和嘘声)。利用生物测定扫描检测。生理反应检测可选择性地监测受试者的心率、血压、瞳孔扩张、体温、心电图和精神活动。活动监视检测器监视参与响应，优选地包括投注率、花在显示器上的时间、保留率、重复率和重复参与率。有利地利用了分析。

[0093]系统的输出用作人工智能或机器学习系统的输入。例如，在神经网络中使用强化学习的训练中，正权重使用 FBR 正属性，负权重使用 FBR 负属性。

[0094]该系统还可以提供被识别为与成瘾(例如赌博成瘾)相关联的输出，或者与以其他方式对游戏上瘾的对象相关联的输出。当参与程度或轻微上瘾被视为可接受时，可在训练中使用正权重，而当上瘾被视为不可接受或过度时，可在训练中使用负权重。

[0095]人工智能、机器学习、神经网络、在训练 AI/ML 系统中使用用户响应(通常图 2)。**11** 和上面的讨论)可以有利地用于游戏设计和开发、娱乐开发和/或任何创造性开发工作。

[0096]这些系统可以构成工具矩阵。它们可以包括一组给定的工具。在更根本的意义上。通过这种方式，它们构成了一个发现工具的工具。工具可以是游戏状态、娱乐状态或任何形式的状态或物质。

[0097]下面将描述游戏开发，但是工具、系统、方法和架构可以应用于娱乐或任何创造性工作。对于特定的游戏，第一个选项是只提供该特定游戏的基本规则。为了发现获胜的游戏策略，该系统可以与其自身对战，或者与其他系统对战。在另一种选择中，可以向系统提供已知的游戏比特，允许系统使用或忽略游戏比特。在又一可选实施例中，该系统可以配备有游戏库。该系统可以分析游戏库、FBR 游戏元素、游戏机制或核心循环。可选地，系统可以将游戏库的分析限制为类似的游戏，或者可以考虑可选地分成子单元的所有游戏，例如纸牌游戏、棋盘游戏、视频游戏。一旦定义了各种核心循环或游戏元素，系统就可以将它们组合成各种组合和排列，以便定义新的游戏或游戏进行序列。系统可以识别数据中的模式。可以将值分配给各个点或游戏状态或游戏状态决策点的决策。用户响应的使用可以有利地用于游戏形成和优化。用户响应的使用特别适合于强化学习。

[0098]该系统可以以分层方式操作。可以使用分级系统，其中它可以改变一个从属强制参数，只要满足“上级”或“主”强制参数即可。举例来说，可以使用‘超级’强制参数‘来保证特定的结果。可替换地，可以授予管理控制，诸如设置‘top LeveF 约束’。

[0099]系统可以考虑合作动作中的单独功能。职能可能会被重新分配或转移到其他(特别是较低的)行动级别。系统可能会提供新的变量。通过提供分层响应，可以维护核心功能。可选地，该系统可以例如基于来自管理员的命令或基于预定义的标准来使用系统的“终止开关”FBR、凋亡。该系统可以提供诸如处于连续状态和/或持续状态的一整套体验(“全面回忆”)。

[0100]无花果。12 和 13 涉及各种动态的、多变的系统。在名称“d-API”和“d-SDK”中，‘d’代表 FBR 4Dynamic‘，并且能够在系统内和由系统进行更改。交互(请求和/或响应)的格式可以是改变。或者，它可以改变响应中提供的信息的类型、数量或质量。其他可能更改的因素包括请求通过 API 或 SDK 更改信息的能力。可以更改其他操作或管理权限，例如只读访问、读写、编辑权限、超级管理权限。这些都提供了自适应控制下的 FBR 动态变化。

[0101]在动态应用编程接口(d-API)内，定义初始格式的 FBR 请求和响应。这可以在 tiSThen，语句中考虑'如果您要求 FBR X 采用商定的格式，则系统将提供 X。动态系统可能会改变格式和/或响应。智能动态更新可以基于人工智能、机器学习或分析。虽然不是。

限于以下，这些改变中的一些或全部可以动态实现：交互的格式(请求和/或响应)、对更多信息或功能的访问(例如只读)或修改权限、向系统提供信息或数据的能力、以及改变数据的能力。

[0102]动态游戏开发工具包(d-GDK)中提供了初始工具包。然后，系统允许动态修改 GDK。优选地，动态修改基于人工智能或机器学习或分析。

[0103]可以提供动态隔离彩票(d-SL)，其中可以提供一个或多个功能单元或彩票。可以使用虚拟化系统，例如在使用虚拟化服务器时。

[0104]无花果。14-20 涉及用于游戏、娱乐或其他有用目的的区块链实现。区块链使用加密的“散列”来识别每个区块和交易。每个连续的块都包含先前代码的散列。这将按时间顺序永久修复事务。区块链同时利用私钥和公钥。将先前的散列与现时值一起添加到新的区块链中，以形成新的散列。

[0105]加密货币提供 FBR 加密安全交易。加密货币是一种可编程货币或分散的价值转移系统。它也是一种去中心化的虚拟货币或去中心化的数字货币。

[0106]工作证明或利害关系证明是参与区块链的“权利”。它必须足够繁重，可以在不重做工作的情况下阻止更改。比特币是一种创造的货币，它被挖掘出来，作为一种奖励，用于 FBR 支付处理工作。区块链加密货币不涉及交易手续费或购买者支付的费用。没有退款权利或退款。

[0107]它可以在任何形式的公共和私有网络中实现。可以使用开放软件和专有软件。存储可以是本地存储或云存储和计算。分析可以在本地或在云分析系统中执行。可以执行分析即服务(AAAS)。系统可以是许可的，而不是无许可的分布式系统。

[0108]无花果。21 至 23 **与**智能合约有关。核心要素是，第一，一套承诺，可以是合同的，也可以是非合同的。其次，它们以数字形式指定，以电子方式运行，其中合同条款或功能成果嵌入代码中。第三，它们包括基于协议或技术的基于规则的操作。第四，当事人通过自动履行承诺，以一般不可撤销的方式履行承诺。

[0109]智能合同可自动执行不同的流程和操作。在一个实施例中，它们在具有终止性自我执行的基础上自动执行 4ISTH-THEN。他们可能会提供 FBR 付款。行动可以以一笔或多笔付款为条件，例如根据付款控制抵押品。

[0110]智能合同可以通过区块链实现。这形成了可在企业对企业实现(B 到 B)和/或对等实现中实现的可信系统。机器对机器的实现允许各种组合。在一个实现中，区块链与构成物联网(LOT)的设备相结合。在另一件事上。结合起来，区块链可以与组成物联网的设备结合起来，与人工智能相结合。通常，该块包含智能合约程序逻辑。它将与特定智能合同相关的消息捆绑在一起，包括输入、输出和逻辑。在又一实施方式中，它们可以提供合约 FBR 差异，例如在使用当前市场价格来调整余额和分散现金流时。**[0111]智**能合约是一种信任转移技术。它们降低了交易对手的风险。最好是，这有助于增加信贷。

[0112]智能合同可以在各种模型中实施。它们可能是一份完全用代码写成的合同。它们可以是具有单独自然语言版本的代码中的合同。它们可以是具有编码性能的分裂的自然语言契约。或者，它们可以是具有编码支付机制的自然语言合同。

[0113]智能合同启动需要达成共识。算法构成合同中的每个参与者如何处理消息的一组规则 FBR。它们可以无许可的方式实现，其中任何人都可以提交消息 FBR 处理。提交者可能参与协商一致。或者，他们可以将决策委托给管理员或参与者子组。另一种实现方式是建立一个允许的系统，其中参与者受到限制。它们通常是预先选定的。然后，他们必须接受门禁进入，并必须满足某些要求和/或管理员的批准。

[0114]智能合同适用于不同的订立方法。他们可以通过协议达成协议，例如在有共同的合作机会或确定的预期结果的情况下。这些可能包括商业惯例、资产互换和权利转让。下一步，条件设置 FBR 合同的启动。这可能是由当事人自己决定的，也可能是由某些外部事件的发生造成的，例如时间、其他可量化的度量或地点。通常，他们会生成一个代码，该代码是用区块链技术加密和链接的。它可以被认证和验证。在执行和处理时，网络更新所有分类帐以指示当前状态。一旦验证并发布，它们就不能更改，只能附加其他块。

[0115]重申一下，智能合同作为具有独立内置信任机制的网络上的分布式应用程序。该方案赋予价值单位结合规则 FBR 转让价值单位的所有权。它们充当自动执行程序，自动满足程序化关系的条款。

[0116]图 3.。20 示出了作为智能合约实现的彩票实施例。实现抽奖的方法 FBR 包括以下步骤。设置接收加密货币的时间范围。第二，在时间范围内接收带有所有者标识的加密货币。窗口在指定的持续时间内打开 FBR，之后窗口关闭。智能合约例如从随机数生成器生成或接收随机事件。随机数生成器应该包括随机性的算法保证和无黑客攻击的保证。合同在所有者标识相关的加密货币中选择新的所有者(赢家)。然后，它将加密货币的新所有权分配给选定的新所有者(获胜者)。

[0117]智能合同可用于实现核心循环或游戏机制。以下核心循环和。

游戏机制包括可以实现的部分列表，包括但不限于 Jacko、Poko、hotSeat、Hi Lo、Rock、Paper Scissor、in the Zone 和 iLotto 或其他基于阵列或地理的游戏机制或核心循环。游戏机械师或核心循环的任何子单元本身都可以用作游戏机械师或核心循环。

[0118]Jacko 是一种游戏，包括以下步骤：从具有最小和最大数字的第一数字范围中随机选择目标数字；向玩家呈现目标数字的指示；选择数字 FBr，该数字从具有最小和最大值的第二范围中选择，其中最大值等于或小于第一范围的最小值切；从玩家接收是否再次抽签的指示；如果是，则从第二范围中随机选择一个数字，累加玩家的总抽签次数，重复该步骤，直到玩家拒绝抽签或者总数超过目标数目，并且在玩家拒绝抽签的情况下，从第二范围中随机选择数字，累加这些数字，将它们与玩家的累积量进行比较，并且分配总数目最接近但不超过目标的获胜者。

[0119]Poko 是一种多人游戏，其中多个标记被授予预定值，而其他玩家没有关于其他玩家持有的至少一些标记的信息。

[0120]高 LO 是一种包括以下步骤的游戏：对一系列随机抽取的数字执行第一次抽奖选择，从玩家接收下一个随机抽取的数字将高于还是低于前一个数字的指示，如果正确，则奖励与随机抽取的数字的数量相关的奖金，并且继续进行，直到玩家无法预测高/低结果，或者选择停止。

[0121]在该区域中是一种碰运气游戏，该游戏包括以下步骤：在预定义的数字范围内随机选择玩家的目标数字，该范围具有最小和最大；随机选择彩票游戏中使用的一系列数字 FBR，该预定义的数字范围的最小值至少等于该系列数字的最低可能总 FBR 和该预定义范围的最大值的和；通过选择的结论对随机选择的一系列数字进行合计，以及根据玩家数量与总数的接近程度，将奖金金额分配给玩家数量不超过总数的玩家。

[0122]石头布剪刀是一种具有三个或更多选项的游戏，这些选项相对于彼此具有指定的选项优先级。

[0123]竞争席位是一种增加风险/回报的游戏，包括在 Smart ContRact 中选择退出的能力。一种在最终级别达到最终级别的多级机会游戏中进行 FBR 游戏的方法，包括以下步骤：在给定级别呈现多个随机选项，其中至少一个选项是正选项，另一个选项是负选项，以及需要进一步决策的第三选项，接收关于选择多个随机选项中的哪一个的选择，以及如果选择了正选项，则将正选项结果与先前正选项结果累加，但是如果选择了负选项，则累加负选项结果，比较累加结果。如果累计次数小于预定次数，则重放相同级别，或者如果累计次数等于预定次数，则终止游戏，并且如果选择了第三选项，则接收关于该决定的选择，尊重上述步骤，直到玩家停止，与发生的预定数量的负面事件或最终级别相关。

[0124]iLotto 是基于网格或地理的系统，包括呈现识别对象的网格的显示 FBR、接收识别对象的玩家选择的输入 FBR、随机选择获胜识别对象的随机生成器 FBR、以及根据规则向玩家奖励积分的计分系统 FBR，所述规则包括：如果玩家选择的识别对象与获胜的识别对象完全匹配，则第一积分值；如果玩家选择的识别对象与获胜的识别对象具有几何关系，则第二积分值；以及如果玩家选择的识别对象与获胜的识别对象具有几何关系，则第二积分值。

[0125]图 3.。23 涉及执行授权参数和可变参数。强制参数在智能合同中设置。强制参数的示例包括支出百分比和支出金额。可变参数受制于强制参数，提供娱乐选项。

[0126]图 3.。24 描绘了用于电子存储加密货币的钱包。这表示图形用户界面，例如电话或计算机显示器上的图形用户界面。各种形式的加密货币可以显示在 GUI 上并存储在钱包中。可以奖励积分，例如 FBR 忠诚度、频率和广播时间。可以列出最近或最近的交易，注明日期、目的和金额。可能会显示总帐户值。

[0127]加密货币系统和智能合约可以与其他系统结合实施。一个额外的系统包括常客或球员的俱乐部系统。它们可能与其他形式的“货币轻量级”相结合，包括微交易和微支付。它们可以与智能资产(即知道其所有者是谁的数字资产或实物)结合使用。数字资产是以数字格式存在的任何东西，通常是二进制格式，并附带使用权。示例包括图像(包括静止图片和视频或动态图像)、可听内容(例如声音、音乐或表演)以及数字文档。所有权通过分布式可信网络控制的财产，例如使用合同的区块链。它们还可以与地理位置结合使用，其中各种组件和建筑组件的物理位置(地理位置)可选地是系统的组件。游戏的地理位置可能会受到限制。该系统可以确保符合数据路由的地理位置。

[0128]无花果。25 至 27 **涉**及具有分离的安全功能和公共功能的系统。这为公共功能和公共实体提供了一个具有多个接口的安全平台。分离的安全功能提供信任代理的功能。安全功能包括以下一项或多项。第一，结果决定。这可能包括使用随机数生成器(RNG)或概率引擎。第二，存储用户或玩家帐户信息。第三，存储货币会计或交易。第四，进行监管和合规接口。第五,。

诸如开发人员界面之类的界面。第六，可以提供问答测试、合规性测试和审批等监管职能。

[0129]公共职能包括以下部分或全部。首先，公共系统向安全系统发出‘呼叫’。调用可以通过应用编程接口(API)或 D-API 进行。“open”系统调用调用保护系统 FBR 安全数据。其次，设计器界面用于访问工具、API、开发工具包(DK)和软件开发工具包(SDK)。第三，市场界面充当彩票界面以及可选的应用程序或应用程序商店。第四，操作员接口用于与操作员或组织者(例如慈善机构)对接。它最好服务于出版、营销和销售。第五，用户界面允许注册、播放活动和持久历史记录。

[0130]系统部件可能因功能不同而不同。公共接口和功能优选地包括“开放”平台。这允许 FBR 仲裁并与安全实体达成关于由安全实体执行的游戏操作的协议，例如，支付百分比、可以玩的 vGLEP 和地理位置。安全实体执行安全功能，包括游戏结果、财务事项和安全用户数据。终端用户利用包括但不限于网络、移动应用、移动网络、平板电脑、计算机、支持显示的设备(无线)、零售商处的触摸屏设备(例如，台面游戏)的“频道混合”。私人实体可以施加速率限制并施加负责任的游戏控制。

[0131]无花果。28 和 **29** 描述了混合和分层系统。诸如国营彩票的集中式系统可以与诸如区块链实现的分散式系统相结合。可以在系统内强加分层顺序。在使用强制和可变参数的系统中，可以建立强制参数的分层结构，然后各种可变参数可以服从适当的强制参数。在另一应用中，可以在层次中的较高级别施加全局使用率限制。可以实施分级使用费率限制。系统的各种拓扑结构包括主从式、主从式和循环式。

[0132]图 3.。30 涉及游戏或彩票关联的信用卡和信用卡功能。信用卡和信用功能可以链接到彩票或其他游戏。通过使用信用卡，建立了转换率。例如，FBR 每 100 美元的购买，1 美元的彩票游戏。费率可以是可变的，例如基于机构。在组织或赞助彩票或游戏的慈善组织中，每购买 100 美元，该组织将获得 2 美元的 FBR。也可以执行拆分，例如信用卡所有者在彩票或游戏中每购买 100 美元可获得 1 美元的 FBR，组织可获得 1 美元的 FBR。

[0133]在替代实施例中，移动游戏设备可以通过电缆连接到游戏机，或者直接连接到游戏机的端口，或者经由与游戏机通信的网络连接到游戏机。

[0134]用于根据这里描述的实施例对游戏机和服务器进行编程的软件最初可以存储在诸如 CD 或电子存储设备的 ROM 上。这样的 CD 和设备是非暂时性的计算机可读介质。存储在其上的适当的计算机指令。该程序也可以通过赌场的网络下载到游戏机上。

[0135]用于根据这里描述的实施例对游戏机和服务器进行编程的软件最初可以存储在诸如 CD 或电子存储设备的 ROM 上。这样的 CD 和设备是其上存储有适当的计算机指令的非暂时性计算机可读介质。该程序也可以通过赌场的网络下载到游戏机上。

[0136]应当理解，这里描述的终端、处理器或计算机可以以多种形式中的任何一种实现，例如机架式计算机、台式计算机、膝上型计算机或平板计算机。此外，计算机可以嵌入通常不被认为是计算机但具有适当处理能力的设备中，该设备包括电子游戏机、网络电视、个人数字助理(PDA)、智能电话或任何其他合适的便携式或固定电子设备。

[0137]此外，计算机可以具有一个或多个输入和输出设备。这些设备尤其可以用来呈现用户界面。可用于提供用户界面的输出设备的示例包括打印机或显示屏、输出的 FBR 可视呈现和输出的扬声器或其他声音生成设备 FBR 可听呈现。可用于用户界面的输入设备的示例包括键盘和诸如鼠标、触摸板和数字化平板的定点设备。作为另一示例，计算机可以通过语音识别或以其他可听格式接收输入信息。

[0138]这样的计算机可以通过任何适当形式的一个或多个网络互连，包括作为局域网或广域网，例如企业网或因特网。这样的网络可以基于任何合适的技术，并且可以根据任何合适的协议操作，并且可以包括无线网络、有线网络或光纤网络。如这里所使用的，术语“在线”指的是这样的联网系统，包括使用例如专用线路、电话线、电缆或 ISDN 线路以及无线传输联网的计算机。在线系统包括使用例如局域网(LAN)、广域网(WAN)、因特网以及上述各种组合的远程计算机。合适的用户设备可以连接到网络 FBR 实例、能够通过网络进行通信的任何计算设备，诸如台式、膝上型或笔记本计算机、移动站或终端、娱乐设备、与显示设备通信的机顶盒、诸如电话或智能电话的无线设备、游戏控制台等。例如，“在线游戏”包括通过互联网上的网站提供的游戏活动。

[0139]此外，这里概述的各种方法或过程可以被编码为可在采用各种操作系统或平台中的任何一种的一个或多个处理器上执行的软件。另外，这样的软件可以使用多种合适的编程语言和/或编程或脚本工具中的任何一种来编写，并且。

还可以编译为在框架或虚拟机上执行的可执行机器语言代码或中间代码。

[0140]在这方面，实施例可以提供编码有一个或多个程序的有形、非暂时性计算机可读存储介质(或多个计算机可读存储介质)(例如，计算机存储器、一个或多个软盘、光盘(CD)、光盘、数字视频盘(DVD)、磁带、闪存、现场可编程门阵列或其他半导体器件中的电路配置、或其他非暂时性、有形计算机可读存储介质)，当在一个或多个计算机上执行这些程序时。计算机可读介质或介质可以是可运输的，使得存储在其上的一个或多个程序可以加载到一个或多个不同的计算机或其他处理器上，以实现如上所述的各个方面。如这里所使用的，术语“非暂时性计算机可读存储介质”仅包括可被认为是制品或机器的计算机可读介质，并且不包括暂态信号。在此使用的术语“非暂时性计算机可读存储介质”仅包括可被认为是制品或机器的计算机可读介质，并且不包括暂态信号。

[0141]这里一般意义上使用的术语“程序”或“软件”指的是可用于对计算机或其他处理器编程以实现如上所述的各个方面的任何类型的计算机代码或计算机可执行指令集。另外，应当理解，根据本实施例的一个方面，当执行执行方法的一个或多个计算机程序不需要驻留在单个计算机或处理器上，而是可以以模块化方式分布在多个不同的计算机或处理器之间，以实现在此描述的实施例的各个方面。

[0142]计算机可执行指令可以是由一个或多个计算机或其他设备执行的多种形式，诸如程序模块。通常，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等。通常，在各种实施例中，可以根据需要组合或分布程序模块的功能。

[0143]此外，数据结构可以以任何合适的形式存储在计算机可读介质中。为简单起见，可以将数据结构示为具有通过数据结构中的位置相关的字段。这样的关系同样可以通过为具有计算机可读介质中的位置的字段分配存储来实现，该计算机可读介质传达字段之间的关系。然而，可以使用任何合适的机制来建立数据结构的字段中的信息之间的关系，包括通过使用指针、标签、地址或在数据元素之间建立关系的其他机制。

[0144]这里描述的实施例的各个方面可以单独使用、组合使用，或者以前述描述的实施例中未具体讨论的各种布置使用，因此这里描述的概念在它们的应用上不限于前述描述或附图中所示的组件的细节和布置。例如，一个实施例中描述的方面可以以任何方式与其他实施例中描述的方面组合。

[0145]此外，这里描述的实施例可以提供一种方法，已经提供了该方法的示例。作为该方法的一部分执行的动作可以以任何合适的方式排序。因此，可以构造以与所示不同的顺序执行动作的实施例，这可以包括同时执行一些动作，即使在说明性实施例中被示为顺序动作。

[0146]虽然已经参考其某些示例性特征描述了实施例，但是本领域技术人员可以对所描述的实施例进行各种修改。这里使用的术语和描述仅用于说明，并不意味着限制。具体地说，尽管已经以示例的方式描述了实施例，但是各种设备将实践在此描述的创造性概念。已经以各种术语描述和公开了实施例，实施例的范围不打算也不应该被认为受其限制，特别是当它们落入这里所附权利要求的广度和范围时，可以由这里的教导建议的其他修改或实施例被特别保留。本领域技术人员将认识到，如以下权利要求及其等价物中定义的那样，这些和其他变体是可能的。尽管出于清楚和理解的目的，通过图示和示例的方式较详细地描述了前述发明，但是根据本发明的教导，本领域的普通技术人员可以很容易地看出，在不背离所附权利要求的精神或范围的情况下，可以对其进行某些改变和修改。

[0147]本说明书中引用的所有出版物和专利在此以引用方式并入，就好像每个单独的出版物或专利被具体地和单独地指示通过引用将其整体并入一样。

参考文献。

[0148]IBM ARM，《2017 物联网商业指数，动态转型》，《经济学人》，智库有限公司 2017，第 1-22 页。

[0149]Crosby 等人的《区块链技术：《超越比特币》，《应用创新评论》，第 2 期，Sutardja Center for EntretreURship&Technology，BerkeLey Engineering，2016 年 6 月，第 1-19 页。

[0150]Fisher，“‘分散式点对点游戏资产平台，使用 Smart ContRact 与第三方游戏集成，’‘。Https://BRavenewcoin.com/assets/Whitepa-。

每个人/。BitSharesPlayWhitePaper-Z.pdf.。2014 年 8 月 4 日。12 页。

[0151]Hinton 等，4《深度信念网络的AFast 学习算法》，神经计算，18,1527-1554,2006。

[0152]Jouppi 等人的《张量处理单元 TM 的数据中心内性能分析》，将于 2017 年 6 月 26 日在加拿大多伦多举行的第 44 届国际计算机体系结构研讨会(ISCA)上发表，第 1-17 页。

[0153]LeCun 等人，《深度学习》，《自然》，第 521 卷，2015 年 5 月 28 日，第 436-444 页。

[0154]Marvin，4<区块链 A-Z：关于比特币背后的改变游戏规则的技术，你需要知道的一切“，...，201.6，6 月 3 日，9 页。你需要知道的关于 https://www.pcmag.com/.../blockchain-A-z-everything--g 的信息。

[0155]Marvin，《区块链：《正在改变世界的无形技术》，2017 年 2 月 6 日，32 页 Http://www.pcmag.com/ar-Ticle/351486。。

[0156]Mougayar，《商业区块链》，第 6-9 ***页，128-133 页。*** 2016 年，由新泽西州霍博肯的 John WiLey&Sons 出版。

[0157]Nakamoto，《比特币-点对点电子现金系统》，citeseerx.ist.psu.edu./viewdoc/SUmmary- ？doi=10.1.1.22.1.9986,2008 页。1-9。

[0158]Ng，4《人工智能现在能做什么和不能做什么》，《哈佛商业评论》，2016 年至 2011 年 /what-Artificial-intelligence-can-And-cant-do--Now，2016 年 11 月 9 日，5 页。Https://hbr.org/。

[0159]O‘Dowd 等人的《IBM’s Open Blockchain，Making BlockChain Real for Enterprise》。IBM 区块链，2016 年 4 月，第 1-20 页。

[0160]Ronan，《深度学习预测 LOTO 数字》，巴黎学院，2016 年 4 月 1 日，第 1-4 页。

[0161]智能合同联盟，“‘智能合同：12 个使用案例 FBR Business and Beyond，A Technology，Legal&Regulatory Information，由智能合同联盟一与德勤(数字商务商会的行业倡议)合作编写，2016 年 12 月，第 1-53 页。

[0162]图灵，《计算机器与智能》，思想 49：1950 年，第 433-460 页。

[0163]伍德，《以太：《安全的分散式通用交易分类账》，宅基地草案，HTTPS：//pdfs.semanticscholar.org/acl5ea808ef3bl7ad754f91d3a. 。00fedc8f96b929.pdf，2014，第 1-32 页。

[0164]Wu 等人的《Google 的神经机器翻译系统：《弥合人机翻译之间的鸿沟》，arxiv：1609.08144v2[cs.CL]2016 年 10 月 8 日，第 1-23 页。

[0165]Yli-HUUmo 等，《区块链技术的当前研究在哪里？--系统评价》，《公共科学图书馆・综合》，DOI ll(10)：e0163477.doi：10.1371/joUmal.pone。0163477,2016 年 10 月 3 日，第 1-27 页。

术语表。

[0166]51%攻击：对比特币网络的攻击，允许攻击者创建欺诈性交易，参见 Double Spend。这是可能的，因为控制了比特币网络 50%以上的哈斯率意味着攻击者可以在计算上胜过所有其他正在挖掘的人。

一个。

[0167]帐户：帐户具有作为以太状态的一部分维护的固有余额和交易计数。它们还具有一些(可能为空)EVM 代码和与其关联的(可能为空)存储状态。虽然是同质的，但区分两种实际类型的帐户是有意义的：具有空的关联 EVM 代码的帐户(因此，帐户余额由某个外部实体控制，如果有的话)和具有非空的关联 EVM 代码的帐户(因此，帐户代表自治对象)。每个帐户都有一个单独的地址来标识它。

[0168]地址：比特币地址用于接收和发送比特币网络上的交易。它包含字母数字字符串，但也可以表示为可扫描的二维码。比特币地址也是公钥。比特币持有者用来对交易进行数字签名的密钥对(参见公钥)。

[0169]地址：用于标识帐户的 160 位代码。

[0170]协议分类帐：协议分类帐是两个或多个当事人用来谈判和达成协议的分布式分类帐。

[0171]空投：一种在人群中分发加密货币的方法，2014 年初首次尝试使用 AURoRaco in(AURoRaco In)。

[0172]算法：在计算或其它解决问题的操作中要遵循的过程或规则，尤指计算机所遵循的过程或规则。

[0173]备用币：作为比特币替代品提供的 FBR 加密货币的统称。莱特币、羽毛币和 PPCoin 都是替代币。

[0174]反洗钱：反洗钱技术被用来阻止人们转换非法获得的资金，使其看起来像是合法赚取的。反洗钱机制本质上可以是法律的或技术的。监管机构经常将 AML 技术应用于比特币交易所。

[0175]App：EtherUm 浏览器中托管的最终用户可见的应用程序。

[0176]应用程序接口(API)：组件(通常是软件组件)用作彼此通信的接口的规范。可以包括规范 FBR 例程、数据结构、对象类和变量。

[0177]套利：通过在同一资产价格不同的市场之间进行交易而产生的无风险利润。

[0178]ASIC：专用集成电路是专门为完成单一任务而设计的硅芯片。就比特币而言，它们旨在处理 SHA-256 散列问题，以挖掘新比特币。

[0179]ASIC Miner：一种包含 ASIC 芯片的设备，用于挖掘 FBR 比特币。它们可以是插入背板的电路板、带有 USB 连接器的设备，也可以是包含所有必要软件的独立设备，这些设备通过无线链路或以太网电缆连接到网络。

[0180]ASIC 挖掘：你在电子商店购买的开箱即用的计算机系统通常不包括加密货币挖掘过程所需的处理能力。因此，许多矿工购买了单独的计算设备，完全搁置了 FBR 挖掘。作为另一种选择，他们也可以得到专用集成电路；这是一种专门设计的计算机芯片，用于执行一种特定的功能，在这种情况下，只有一功能，即挖掘计算。ASIC 降低了 FBR 开采所需的处理能力和能源，并可以通过这种方式帮助降低整个过程的成本。无论专用集成电路一(专用芯片本身的术语)是集成到现有的计算系统中，还是作为独立设备运行，术语“专用集成电路”。通常指的是整个系统本身，而不仅仅是芯片。

[0181]非对称密钥算法：这是用于生成公钥和私钥的算法，公钥和私钥是加密货币交易必不可少的唯一代码。在对称密钥算法中，发送方和接收方都拥有相同的密钥：它们可以私密地加密和交换信息，但是由于双方都拥有解码信息，所以它们不能对彼此保密。

使用非对称密钥算法，双方都可以访问公钥，但只有拥有私钥的人才能解密加密；这确保了只有他们才能收到资金。

[0182]证明台账：一种分布式分类帐，提供协议、承诺或声明的持久记录，提供这些协议、承诺或声明已作出的证据(证明)。

[0183]自治代理：在没有人工干预的情况下做出决策并对其采取行动的软件。

[0184]自治对象：仅存在于假设的以太状态中的虚构物体。有一个内部地址，因此有一个关联的帐户；该帐户将具有非空的关联 EVM 代码。仅作为该帐户的存储状态合并。

B 类。

[0185]基数 58：Base58 将二进制数据编码为文本，并用于编码比特币地址。由中本聪(Satoshi Nakamoto)创建，其字母数字字符不包括“0”。“O”、“1”、“I”，因为它们很难区分。

[0186]Base58 检查：Base58 的变体，用于检测比特币地址中的键入错误。

[0187]捕熊器：这是投资者对股票或商品的操纵。“设置”熊市陷阱的交易员通过抛售股票，直到它让其他投资者认为其价值上升趋势已经停止或正在下降。那些落入熊市陷阱的人往往会在那个时候抛售，因为他们担心价值会进一步下跌。在这一点上，设置陷阱的投资者将以低价买入，并将释放陷阱-这本质上是一个虚假的熊市。一旦释放了捕熊器，价值就会持平，甚至会攀升。

[0188]BIP：“比特币改进建议”的首字母缩写，任何想要改善比特币网络的人都可以提交。

[0189]位：比特币面值的名称，等于 100 Satoshis(1 比特币的**百**万分之一)。2014 年，包括比特币(Bitpay)和 Coinbase 在内的几家公司以及各种钱包应用程序都采用了 BIT 来显示比特币金额。

[0190]比特币(大写)：众所周知的加密货币，基于 ProoSof-Work 区块链。

[0191]比特币(小写)：比特币账本使用的具体技术集合，一种特殊的解决方案。请注意，货币本身就是这些技术之一，因为它为矿工提供了开采的动力。

[0192]比特币(货币单位)：一亿，000,000 个智士。一种分散的数字货币单位，可以用来交易商品和服务。比特币也是替代货币生态系统中的一种储备货币。

[0193]比特币 2.0：比比特币白皮书提出的基本支付系统应用更高级或更复杂的比特币或区块链技术的 FBR 应用。比特币 2.0 项目的例子包括对手方、以太、Blockstream、Sarm、Domus 和 Hedgy。

[0194]比特币自动取款机：比特币自动取款机是一种实体机器，允许客户用现金购买比特币。有很多制造商，其中一些可以让用户出售比特币 FBR 现金。它们有时也被称为“BTM”或“比特币 AVMS”。CoinDesk 维护着一张运营比特币 ATM 机的全球地图和一份制造商名单。

[0195]比特币核心：自 2014 年 3 月 19 日发布 0.9 版以来，比特币 Qt 的新名称。不要与 2013 年 8 月发布的 Objective-C 实现 Core 比特币混淆。

[0196]Bitcoind：使用命令行界面的比特币的原始实现。目前是 BitcoinQt 项目的一部分。根据 UNIX 传统，“D”代表 FBR“守护进程”，用于命名后台运行的进程。

[0197]比特币销毁天数：对“比特币网络货币流通速度”的估计。之所以使用比特币，是因为它赋予了很长时间没有使用 FBR 的比特币更大的权重，而且比起每天的总交易量，它更好地代表了比特币正在进行的经济活动水平。

[0198]比特币投资信托基金：这一私人的开放式信托专门投资于比特币，并代表其股东使用最先进的协议来安全地存储比特币。它为 FBR 的人们提供了一种投资比特币的方式，而不必自己购买和安全地存储这种数字货币。

[0199]比特币 J：迈克·赫恩的完整比特币节点的 Java 实现。除其他功能外，还包括 SPV 实现。

比特币 JS：

[0200]一个使用 FBR 比特币开发的在线 Javascript 代码库，特别是网络钱包、bitcoinss.o 昭()。Http://bitcoinjs.org。

[0201]比特币市场潜力指数(BMPI)：比特币市场潜力指数(BMPI)使用一个数据集对 177 个国家的比特币潜在效用进行排名。它试图展示哪些市场最有潜力采用 FBR 比特币。

[0202]比特币网络：维护区块链的分散的点对点网络。这是处理所有比特币交易的工具。

[0203]比特币价格指数(BPI)：CoinDesk 比特币价格指数代表了符合 BPI 指定标准的全球领先交易所的比特币价格平均值。还有一个 API FBR 开发者可以使用。

[0204]比特币协议：一种开放源码的密码协议，在比特币网络上运行，设定网络如何运行的“规则”。

[0205]BitcoinQt：比特币 Qt 是您的计算机使用的开源软件客户端。它包含区块链的副本，一旦安装，它就会把你的电脑变成比特币网络中的一个节点。还充当“桌面钱包”。**[0206]比特币**-红宝石：朱利安·朗沙德尔(Julian Langschaedel)在鲁比的比特币公用事业图书馆。在 Coinbase.com[0207]比特币情绪指数(BSI)上用于生产：比特币情绪指数是一项衡量个人在任何一天感觉这种数字货币的前景是上升还是下降的指标，该指数是由 Qrious 收集的数据提供支持的。**[0208]比特**币白皮书：这份比特币白皮书是由中本聪(Satoshi Nakamoto)撰写的，并于 2008 年发布在加密技术的邮件列表上。本文详细介绍了比特币协议，值得一读。中本聪(Satoshi Nakamoto)紧随其后，于 2009 年发布了比特币代码。

[0209]比特币白皮书：2008 年 11 月，一篇由中本聪(Satoshi Nakamoto)撰写(很可能是化名)的论文发布在新创建的 Bitcoin.org 网站上，标题为“比特币：一个点对点的电子现金系统。这份长达八页的文件描述了使用点对点网络生成“FBR 电子系统”的方法。

不依赖信任的交易“，并规定了加密货币的工作原理。

[0210]位核：Bitpay 用 JavaScript 编写的比特币工具包。比比特人更完整。

[0211]BitPay：一种比特币支付处理器，它与商家合作，使他们能够接受比特币作为支付。

[0212]BitStamp：一种越来越受欢迎的 FBR 比特币交易所。阅读最新的 BitStamp 新闻。

[0213]区块：这是交易数据的集合，是加密货币的基本要素之一。在进行交易时，会收集每个交易的相关信息 FBR-当收集到的数据达到预定大小时，就会将其捆绑成一个块。区块创建后，尽快由投资者进行 FBR 交易验证；这一过程称为挖掘。

[0214]区块链：自比特币加密货币开始以来已挖掘的块的完整列表。区块链的设计使得每个区块都包含在其之前的区块上的哈希图。这是为了使它更好地防篡改而设计的。更让人困惑的是，还有一家名为 BlockChain 的公司，该公司拥有非常受欢迎的区块链浏览器和比特币钱包。

[0215]区块减半：[参见减半]矿工在开采一个区块时获得的比特币奖励减半。这大约每 4 年发生一次(准确地说是每 210,000 个区块)。

[0216]块头：包含有关块的信息，如前一个块标头的散列、其版本号、当前目标、时间戳和随机数。

[0217]区块高度：区块高度是指区块链中连接在一起的区块数量。例如，高度 0 将是第一个块，也称为创世纪块。

[0218]Blockchain.infb：一种运行比特币节点并显示所有交易和块的统计数据和原始数据的 Web 服务。它还为轻量级客户端 FBR Android、iOS 和 OS X 提供网络钱包功能。

[0219]整体奖励：对成功散列事务块的矿工的奖励。这可能是硬币和交易费的混合，这取决于相关加密货币使用的策略，以及是否所有硬币都已成功开采。比特币目前每个区块奖励 25 个比特币 FBR。当一定数量的区块被开采时，区块奖励减半。以比特币为例，门槛是每 21 万个区块。

[0220]引导：FBR 技术通过几条简单的指令将程序上传到志愿者的计算机或移动设备上，从而启动程序的其余部分。

[0221]BOT 交易：在交易平台上运行的软件程序，通过预先编程的交易指令执行买入和卖出指令。

[0222]大脑钱包：[见钱包]一种比特币钱包，它使用一长串单词来保护其硬币。这个“口令”是可以记住的，让钱包所有者只需记住口令就可以花掉比特币。

[0223]BRainwallet.org：基于比特币的实用程序，可以手工进行交易，将私钥转换为地址，并使用大脑钱包。

[0224]BTC：短货币缩写 FBR 比特币。

[0225]气泡：当投资者推动市场上涨时，泡沫就会出现；在过去十年左右的时间里，互联网和房地产行业就发生了这种情况。行业人气、对潜在价值的投机、政治影响力和许多其他因素可能共同造成这些价值的飙升。如果市场被认为已经“触顶”，或者投资者认为它将不再保持整体价值，泡沫可能会“破裂”。这代表了投资者的大规模抛售，这可能导致市值大幅缩水。根据你的观点，一些加密货币市场可能经历过周期性泡沫，也可能没有经历过周期性泡沫。该行业的反对者坚称，市场波动太大，将继续起伏不定，看不到真正稳定的迹象。相反，业内人士声称，这些都是一个新领域的成长之痛，随着时间的推移，数字货币的波动将会平息下来。

[0226]捕牛器：牛市陷阱是指股票或商品的投资者为了人为地推高价值或制造假牛市而大量买入的人设的陷阱。被牛市陷阱愚弄的交易员通常会以虚高的价格买入股票，因为他们相信上升趋势将继续下去，他们正在购买的股票将会升值。不幸的是，那些落入牛市陷阱的人往往会持有他们支付了太多的股票 FBR，因为一旦陷阱被释放，市场就会平息，有时甚至会下跌。

[0227]梧桐木：这是一个由比特币爱好者 Josh Rossi 创立的项目，目的是在纽约联合广场建立一个公众强烈抗议的比特币交易所。以梧桐木协议命名，该协议形成了 1792 年纽约证券交易所 FBR 的基础。

[0228]购买订单：当投资者接近交易所并想要购买加密货币时，就会建立买入订单。这些订单可以是非常简单的订单(“我想在比特币上花费 x 美元”)，也可以是复杂的订单，包括订单应该完成的时间范围、价格范围等因素。大多数交易所允许 FBR 在线输入这些信息，但一些投资者更喜欢直接与交易所代表讨论细节。买入订单并不一定能保证你的购买；如果你的价格太低，比如 FBR，除非你做调整，否则优惠可能会过期而没有得到满足。

C。

[0229]烛台图：这是一种流行的一目了然的图表，通常用于股票和商品交易所。一些图表使用一个点来显示某一特定股票或商品在某一天的收盘价；虽然这是有价值的信息，但它并不显示商品在交易日中经历的价格范围。在烛台图中，竖线用来显示一个交易日的活动范围；竖线的上边缘将是开盘价(在熊市中)，下边缘表示收盘价(也是在熊市中；在牛市中，两者相反)。线条从顶部和底部延伸出来，显示了当天商品 FBR 的最高和最低交易价格(从而形成了蜡烛的“灯芯”)。烛台图是显示日常市场活动的理想 FBR，以简明但仍然准确的方式显示，表明了这一时期的所有活动 FBR。

[0230]资本管制：这些是地方措施，如交易税、限制或其他禁令，政府可以用来管制资本市场流入和流出该国的资金。

[0231]卡萨西乌斯硬币：由迈克·考德威尔生产的实物收藏币。每枚硬币在防篡改的全息图下都包含一个私钥。“Casascius”这个名字是由一个短语“直言不讳”组成的，这是对比特币本身名字的回应。

[0232]总账：中央分类帐是指由中央机构管理的分类帐。

[0233]更改：非正式名称 FBR 交易输出的一部分，在花费该输出后作为“更改”返回给发送方。由于交易输出不能部分花费，所以人们只能将 3 个 BTC 输出中的 1 个 BTC 用于创建两个新输出：一个是将 I 个 BTC 发送到收款人地址的“付款”输出，另一个是将剩余的 2 个 BTC(减去交易费)发送到付款人地址的“更改”输出。BitcoinQt 总是使用密钥池中的新地址，以获得更好的私密性。Blockchain.infb 会发送到钱包中的默认地址。在使用纸质钱包或大脑钱包时，一个常见的错误是将交易更改到不同的地址，然后不小心将其删除。例如，当在临时比特币 QT 钱包中导入私钥时，进行交易，然后删除该临时钱包。

[0234]检查点：块的散列，在此之前，BitcoinQT 客户端在不验证数字签名 FBR 性能的情况下下载块。检查点通常指的是一个非常深的块(至少有几天)，每个人都清楚该块已被绝大多数用户接受，并且重组不会超过该点。它还有助于保护历史上的大部分内容免受 51%的攻击。由于检查点会影响主链的确定方式，因此它们是协议的一部分，必须由替代客户端识别(尽管通过检查点进行重组的风险非常低)。

[0235]圆：Circle 是一项兑换和钱包服务，为全球用户提供存储、发送、接收和交换比特币的机会。

[0236]客户：在台式机、膝上型计算机或移动设备上运行的软件程序。它连接到比特币网络并转发交易。它还可能包括一个比特币钱包(见 Node)。

[0237]云：参考互联网和它可以执行 FBR 任何人的功能，如存储、文件发送和使用应用程序。

[0238]云哈希/挖掘：一种挖掘类型，人们可以付费从云中的其他人那里租用计算机能力，以挖掘比特币或其他加密货币。这是通过出售采矿合同来实现的。CloudHash 也是提供这项服务的企业的名称。

[0239]硬币：一个非正式的术语，意思是 **1** 个比特币，或者是可以花掉的未花掉的交易产出。

[0240]钱币年代：硬币的年龄，定义为货币数量乘以持有期。

[0241]Coinbase：另一个名字 FBR 是比特币生成交易中使用的输入。当比特币被开采时，它不是来自另一个比特币用户，而是作为对矿工的奖励。这笔奖励被记录为一笔交易，但一些随机数据被用作输入，而不是另一个用户的比特币地址。Coinbase 也是比特币钱包服务的名称，该服务也提供支付。为 FBR 商户提供处理服务，并充当 FBR 从交易所购买比特币的中介。

[0242]Coinbase.com：总部设在美国的比特币/美元兑换和网络钱包服务。

[0243]冷藏：存储私钥的最安全方式是将它们保存在“冷存储”中，使其离线。这可以是硬件钱包、U 盘或纸质钱包的形式。这些钱包被称为“冷钱包”。

[0244]集体开采：在挖掘数字货币数据块的过程中投入资源和材料往往被证明是太昂贵的 FBR 个人无法参与的。因此，许多有进取心的企业已经想出了一种方法，让那些原本会被排除在外的矿工更容易负担得起采矿费用。这些公司投资于允许 FBR 高端采矿电力的硬件，然后将这种采矿能力的使用权出租给第三方。作为一名个人矿工，这意味着你可以签署一份合同，允许你通过云计算使用预定数量的采矿能力，而不需要购买或维护这样做所需的处理能力的麻烦或费用。成功挖掘数据块所带来的块奖励将归从集体采矿公司购买合同的个人矿工。

[0245]彩色硬币：拟议的 FBR 比特币附加功能，使比特币用户能够赋予他们额外的属性。这些属性可以是用户定义的，使您能够将比特币标记为股票份额或实物资产。这将使比特币能够作为代币、FBR 和其他财产进行交易。

[0246]压缩大小：事务和块序列化中使用的可变长度整数格式的原始名称。也被称为“智史的编码”。它使用 1、3、5 或 9 字节表示任何 64 位无符号整数。小于 253 的值用 1 个字节表示，字节 253、254 和 255 表示后面的 16 位、32 位或 64 位整数。较小的数字可以用不同的方式表示。在比特币-红宝石中，它被称为“var_int”，在 Bircoinj 中，它被称为 varint。BitconQT 还有更紧凑的表示形式，称为 Varint，它与 CompactSize 不兼容，用于块存储。

[0247]确认：将比特币交易成功地散列到交易块中，并巩固其有效性的行为。一次确认大约需要 10 分钟，这是对一个事务块进行散列的平均时间长度。然而，一些更敏感或更宽松的交易可能需要多次确认，这意味着在交易的区块被散列后，必须对更多的区块进行散列，并将其添加到区块链中。每次在交易的区块之后向区块链添加另一个区块，交易就会再次得到确认。

[0248]确认号：确认号是对交易可能被主链拒绝的概率的度量。“Zero Confirmations‘’表示交易未确认(还没有在任何区块中)。一个确认意味着该交易包含在主链中的最新区块中。两次确认意味着该交易包含在紧挨着最近一笔交易的区块中。事务被反转(“双重花费”)的概率随着“上面”添加更多的块而呈指数级递减。

[0249]已确认交易：已包含在区块链中的交易。

[0250]交易被拒绝的概率是通过多次确认来衡量的。

[0251]共识要点：一个时间点，或者根据要添加到分类帐中的一组记录数量或数量定义的点，同行在此会面以就分类帐的状态达成一致。

[0252]协商一致进程：负责维护分布式分类帐的一组同行用来就分类帐的内容达成共识的过程。

[0253]延续图模式：当您查看数字货币交易所网站上的市值图表时，您将能够一目了然地看到向上(“牛市”)和向下(“熊市”)的趋势线。然而，有时你会看到一些图形模式，它们显示的波动与当前趋势的流动背道而驰，只是之后趋势继续朝着同一个方向发展。这种类型的图表模式被称为“同质化”类型；尽管一种货币的价值可能会有短暂的上下波动，但从宏观角度来看，趋势并没有真正改变方向。延续图模式显示，投资者已经测试了当前的趋势，并发现它是合理的一，因此，它继续说。

[0254]合同：非正式术语用于表示可能与帐户或自治对象相关联的一段 EVM 代码。

[0255]核心开发人员：开发比特币开源源代码的程序员。他们没有正式受雇于比特币网络，也没有被比特币网络支付费用，也不控制比特币网络；但是，他们在比特币网络的 GitHUb 资源页面上拥有更高的访问权，比特币网络的主要“参考”版本就是在这里开发的。

[0256]造假：为了实施欺诈行为而模仿某物的行为。这方面的一个例子是用假币购物。

[0257]CPU：中央处理器--计算机的“大脑”。在早期，这些工具被用来对比特币交易进行散列，但现在已经不够强大了。它们有时仍被用来散列替代币的交易。

[0258]克雷格·斯蒂芬·赖特：比特币和区块链背后最大的谜团是谁撰写了臭名昭著的 2008 年白皮书，也就是笔名中本聪(Satoshi Nakamoto)背后的真实身份。最近，这场徒劳无功的追逐集中在澳大利亚程序员兼企业家克雷格 •斯蒂芬 •赖特(CRaig Stephen Wright)身上，尽管仍有很多人猜测赖特是真的还是精心设计的骗子(特别是因为他拒绝证明这一点)。寻找区块链之父的工作似乎仍在继续。

[0259]众包：为实现一个目标而汇集的资源，如由普通民众贡献的信息或金钱。这通常是通过人们可以捐赠的网站在网上完成的。

[0260]加密货币：一种仅基于数学的货币形式。与印刷的法定货币不同，加密货币是通过基于密码学解决数学问题而产生的。

[0261]密码学：使用数学来创建可用于隐藏信息的代码和密码。将用于验证和保护比特币交易的数学问题用作基础 FBR。

[0262]CSRNG：首字母缩写 FBR“加密安全随机数生成器”，用于生成私钥 FBR 比特币钱包。

[0263]杯柄：当投资者想要测试大宗商品市场上涨趋势或“看涨”趋势的有效性时，这是一种出现在市值图表上的模式。由于投资者的买入和卖出，这一上升趋势将。逐渐向下倾斜，然后再向后倾斜，呈缓坡的“字母 U”形。在这个“杯子”形成之后，市场将再次进行短暂的测试，形成一个比它前面的“杯子”小得多(持续时间也更短)的快速下行坡度：这就形成了茶杯形状的“把手”。杯子和手柄被认为是一种“同质化”的模式，因为一旦手柄形成，上升的趋势将继续下去。

[0264]旋风：由公司通过水力压裂数字世界 FBR 他们的数据创建的。

D。

[0265]DAO：首字母缩写 FBR“分散的自治组织”，一个理论上的公司，可以存在于云中，并根据预设的算法开展业务，不需要人工管理。也称为“DAC”。

[0266]黑暗使者：Darksend 是黑币的去中心化混合实现，旨在为黑币用户提供更大的交易隐私/匿名性。

[0267]日间交易：这是买入和/或卖出股票或商品的做法，交易的整个过程都在同一个日历日内进行。日间交易者看着 FBR 每分钟的微小价格变动，并通过每天进行几笔交易来尽最大努力最大化他们的利润(或至少将损失降至最低)-但不会留下任何一夜未完成的业务。与普通交易者相比，日内交易者依赖于“微观趋势”，这是市值的微小变化，普通交易者可能会在采取行动之前观察股票或商品的几天、几周或几个月的走势。

[0268]DDoS：分布式拒绝服务攻击使用攻击者控制下的大量计算机来耗尽中心目标的资源。它们通常通过 Internet 发送少量网络流量，以占用目标的计算和带宽资源，从而阻止其向合法用户提供服务。比特币交易所有时会受到 DDoS 攻击。

[0269]死猫弹跳：在市场交易中，这个有点令人不快的短语与一种股票或大宗商品(如加密货币)在下跌趋势中的短暂复苏有关。当出现熊市--也就是说，一种商品的价值在稳步下跌的市场--有两种类型的复苏。第一种类型是真正的复苏，即在很长一段时间内，下行趋势得到逆转，价格持续上行。第二种是“死猫反弹”，价格走势--已经下降了很长一段时间的 FBR--短暂上行，通常 FBR 最多不会超过一到两周。死猫反弹可以是微型的--持续几个小时或几天--但大多数分析师认为这个版本只是市场上的一个小现象，而不是称之为“真正的”死猫反弹。无论反弹持续多久，这都是一种虚假的复苏，之后估值的下降趋势仍在继续。这个词来自一句古老的一，有点令人不安的一说，“即使是一只死猫，如果它从很高的高度坠落，它也会反弹。”

[0270]分散：这是一个在讨论加密货币时经常听到的术语。在这种情况下，这意味着货币不是由银行或政府等中央机构发行或控制的。虽然这意味着加密货币不会直接受到通胀或政府监管的影响-其倡导者坚持认为，这使联邦储备银行成为一个更公平的国际竞争环境一，但这也意味着它的。

投资者对其福祉负有更多责任。他们应该意识到加密货币固有的风险，例如价值波动和缺乏防止盗窃和欺诈的制度保护。FDIC FBR 数字货币一不像美国中央银行系统一那样存在，所以一旦被盗，它就永远消失了。

[0271]深网：没有被搜索引擎索引的在线内容使得访问变得困难。互联网上的大部分内容都驻留在深网上，可以使用一种名为 TOR 的程序进行访问。

[0272]通货紧缩：随着时间的推移，一个经济体中价格的下降。当商品或服务的供应量增长快于货币供应量时，或者当货币供应量有限并减少时，就会发生这种情况。这导致每单位货币有更多的商品或服务，这意味着购买这些商品或服务所需的货币更少。这也有一些不利之处。当人们预计价格会下跌时，这会导致他们停止消费，囤积资金，希望他们的钱以后会走得更远。这可能会抑制经济。**[0273]滞期**费：某些货币惩罚用户囤积 FBR，这是通过滞期费完成的，滞期费是持有未花掉的硬币的 FBR 连锁费用。这项费用会随着时间的推移而增加。**[0274]拒绝**服务[DoS]：是对网络的一种攻击形式。比特币节点通过 24 小时禁止其 IP 地址 FBR 来惩罚其他节点的某些行为，以避免 DoS。此外，一些理论上的攻击，如 51%的攻击，可能被用于 FBR 网络范围的 DoS。

[0275]深度：深度指的是区块链中的一个位置。一笔有 6 个确认的交易也可以称为“6 个街区深”。

[0276]桌面钱包：在您的计算机上存储私钥的钱包，它允许您消费和管理比特币。

[0277]确定性钱包：一种基于从称为种子的单个起始点派生多个密钥的系统的钱包。如果钱包丢失，该种子就是恢复钱包所需的全部，并且可以允许在不知道私钥的情况下创建公共地址。

[0278]难度：此数字决定了对新数据块进行散列的难度。它与事务块散列的给定数值部分中允许的最大数量有关。数字越小，生成适合它的散列值就越困难。难度因矿工在比特币网络上使用的计算能力而异。如果 la 昭 e 数量的矿工离开一个网络，难度将会降低。然而，到目前为止，比特币越来越受欢迎，吸引了更多的计算能力到网络上，这意味着难度增加了。

[0279]数字证书：没有加密-解密操作但用户必须申请(并支付年费)FBR 个人证书的代码片段，大多数常见的电子邮件服务都不支持它们(谷歌、Outlook、雅虎)。

[0280]数码商品：数字商品是一种稀缺的、可电子转让的、无形的、有市场价值的商品。

[0281]数字标识：数字身份是个人、组织或电子设备在网络空间采用或声称的在线或联网身份。

[0282]分布式自治企业[DAE]：几乎不需要或根本不需要传统的管理或层级来创造客户价值和所有者财富。

[0283]分布式应用程序[DAPP]：一套智能合约，将数据存储在房屋列表区块链上。

[0284]分布式资本主义：降低参与门槛。

[0285]分布式台账：分布式分类帐是一种分布在多个站点、国家或机构的数据库。记录一个接一个地存储在连续分类帐中。分布式分类帐数据可以是“允许的”或“不允许的”，以控制谁可以查看它。

[0286]双层底纹：当投资者买入和卖出以测试价值下降趋势时，市场图表上就会形成双底模式。买入和卖出将会发生，随着时间的推移，这将在图表的趋势线上形成两个截然不同且几乎相等的山谷。一旦第二个谷地形成，上升趋势将超过模式形成过程中形成的山峰或顶部的点。一旦发生这种情况，市场很可能会在一段时间内“看涨”，或上升趋势，FBR；因此，双底模式被认为是一种“反转”模式，从熊市过渡到牛市。

[0287]双倍支出：花两次比特币的行为。当某人使用比特币进行交易，然后使用相同的比特币从另一个人那里进行第二次购买时，就会发生这种情况。然后，它们说服网络的其余部分仅通过在块中散列来确认其中一项交易。由于比特币网络的运营方式，双重支出并不容易做到，但对于那些接受零确认交易的人来说，这仍然是一个风险。

[0288]双项图案：当投资者买入和卖出以测试价值上升趋势时，市场图表上就会形成双顶模式。买入和卖出将会发生，随着时间的推移，这将在图表的趋势线上形成两个截然不同且几乎相等的峰值。一旦第二个峰值形成，下跌趋势将在形态形成过程中形成的凹点或谷点之后展开。一旦发生这种情况，市场很可能会在一段时间内“看跌”或下跌，即 FBR；因此，双顶形态被认为是一种“反转”形态，从牛市过渡到熊市。

[0289]灰尘：交易产出小于花费它所需的典型费用[原文如此]。这不是协议的严格部分，因为任何大于零的值都是有效的。BitcoinQt 拒绝挖掘或中继“灰尘”事务，以避免无用地增加未用事务输出(UTXO)索引的大小。

[0290]粉尘交易：一笔交易的比特币数量极少，几乎没有经济价值，但在区块链中占据了空间。比特币开发团队已经努力通过提高网络转播的最低交易额来消除灰尘交易。

E。

[0291]ECDSA：椭圆曲线数字签名算法是用于对比特币协议中的交易进行签名的轻量级加密算法。

[0292]椭圆曲线算法：在二维椭圆曲线上的一组点上定义的一组数学运算。比特币协议使用预定义曲线 secp256kl。以下是对这些操作最简单的解释：您可以将点加减，然后再乘以一个整数。除以整数在计算上是不可行的(否则加密签名将不起作用)。私钥是 256 位整数，公钥是。

该整数的预定义点 G(“生成器”)：A=G*a。结合性定律允许实现有趣的密码方案，如 Diffie-Hellman 密钥交换(ECDH)：具有私钥 A 和 B 的双方可以交换他们的公钥 A 和 B 以计算共享秘密点 C：C+A*b=B*a，因为(G*a)*==(G*b)*a。该点 C 可以用作 AES 加密密钥来保护它们的通信信道。

[0293]企业参与者：区块链开始在企业软件市场产生严重的噪音，IBM 和微软等公司在 Visual Studio、Microsoft AzURe$14,3000.00 和其他云平台等开发者环境中利用 EtherUm。物联网(LOT)技术等。EtherUm 的区块链应用平台在很大程度上一直是门户，但科技巨头现在坚定地进入了区块链业务。集体银行和金融行业也在拥抱以智能合约形式进行的区块链交易。

[0294]4 娱$^{\text{乐}}$：状态、显示、用户体验、刺激(光、声、触觉)、标题 A/价值转移、游戏[0295]托管：在异步交易期间将资金或资产存放在第三方账户中以保护它们的行为。如果 Bob 想把钱寄给 Alice in Exchange FBR 一个文件，但他们不能亲自进行交换，那么他们怎么能信任对方同时把钱和文件寄给对方呢？相反，Bob 将钱发送给 Eve，Eve 是一个信任方，在 Bob 确认他从 Alice 那里收到文件之前，Eve 一直持有资金。然后她把钱寄给爱丽丝。

[0296]ETF：首字母缩写 FBR“交易所买卖基金”。这些是在股票市场交易的投资基金，跟踪标的资产的价格指数。

[0297]以太浏览器：(也称为 EtherUm Reference Client)类似于简化浏览器(A La Chrome)的界面的跨平台 GUI，它能够托管后端完全基于 EtherUm 协议的沙盒应用程序。

[0298]以太运行时环境：(也称为 ERE)提供给在 EVM 中执行的自治对象的环境。包括 EVM，还包括 EVM 所依赖的世界状态的结构 FBR 某些 I/O 指令，包括 CALL&CREATE。

[0299]以太虚拟机：(也称为 EVM)构成执行模型 FBR 帐户的关联 EVM 代码的关键部分的虚拟机。

[0300]EVM 组件：EVM 代码的人类可读形式。

[0301]EVM 代码：EVM 可以本机执行的字节码。用于向帐户正式指定消息的含义和后果。

[0302]交换：交换不同形式的货币和其他资产的中心资源 FBR。比特币交易所通常用于交换加密货币 FBR 和其他通常为法定货币的货币。

[0303]汇率：对于传统货币，这个术语指的是一种政府发行的货币对另一种货币的相对价值。例如，如果你是一个美国人，想从英国的一个商人那里买东西，那么在买东西之前，你应该先看看美元和英镑之间的汇率。这样一来，你就可以准确地知道你将用你的货币支付多少钱，因为它适用于另一种货币。由于加密货币本质上是国际的，无论你在哪个国家，都具有相同的价值，所以这个术语“汇率”有不同的含义。对于数字货币，它可能意味着以下两种情况之一：比特币与美元等传统货币相比如何，或者与另一种加密货币(如比特币与莱特币)相比有何不同。

[0304]外部执行者：能够连接到以太节点，但在以太世界之外的人或其他实体。它可以通过存放签署的交易，检查区块链和关联状态，与以太互动。具有一个(或多个)内部帐户。

[0305]额外的随机数：放置在 Coinbase 脚本中的一个数字，每次现时值 32 位整数溢出时由挖掘器递增。当随机数溢出时，这不是继续挖掘所必需的方式，还可以改变事务的 Merkle 树或改变 FBR 使用的公钥，以获得块奖励。

F。

[0306]水龙头：第一次发射替代币时使用的一种技术。预先开采一定数量的硬币，并免费赠送 FBR，以鼓励人们对这种硬币感兴趣，并开始自己开采。

[0307]费用：请参阅交易费。

[0308]法定货币：一种凭空创造出来的货币，它之所以有价值，是因为人们说它有价值。由于已知它在洗钱和恐怖活动中的应用，它一直受到监管机构的密切关注。不要与比特币混淆。

[0309]填充或封堵：这是一种使用加密货币交易所发出的简单类型的购买订单。投资者决定他们想要多少货币，以什么价格，并确定订单的截止日期 FBR。然后，交易所将根据这些标准尽最大努力完成订单。如果交易所在截止日期前没有找到合适的匹配 FBR 订单，则订单将被取消且未完成。换句话说，根据这些指导原则并在此时间范围内填写此订单。如果你做不到，就杀了它。

[0310]FinCEN：美国财政部下属的金融犯罪执法网络。到目前为止，FIN-CEN 是对交易所比特币交易实施监管的主要组织。

[0311]旗帜图案：当投资者想要测试一种商品价值的当前趋势时，这种模式就会出现在市场价值图表上。在测试期间发生的买入和卖出-通常持续一到三周-一形成的波动可以被平行的对角线包围，形成“：FLAG”的形状。在上升趋势(“熊市”)和下降趋势(“牛市”)期间都可能出现旗型模式。因为它们并不意味着当前的趋势将会逆转，所以旗帜图案被认为是“持续”图案类型之一。一旦格局形成，趋势将继续朝着之前的方向发展。

[0312]方塔斯：与其说这是一个“什么”，不如说是一个“谁”。丰塔斯是一个神秘的投资者或一群投资者，他们一直在利用哄抬和抛售计划来操纵各种数字货币的价值。也就是说，他/她/他们一直在低价大量买入货币，然后他们利用误导性的信息让其他投资者买入，虚假地抬高了货币的价格。在这一点上，丰塔斯出售了他们的加密货币投资中的一大部分，获得了可观的利润。到目前为止，丰塔斯的重点一直是比特币，但他们正试图对 Litecoin 和 Namecoin 做同样的事情；然而，投资者关注的是比特币。

计划。不用说，丰塔斯并不是另类货币行业最受欢迎的投资者。然而，即使是没有被丰塔斯骗局蒙骗的精明投资者也不得不勉强承认它的虚伪。

[0313]叉子：区块链的替代持续版本的创建，通常是因为一组挖掘器开始对一组与另一组不同的事务块进行散列。这可能是恶意造成的，可能是一群矿工获得了对网络的过多控制(参见 51%的攻击)，可能是由于系统中的一个漏洞，也可能是由于核心开发团队决定在新版本的客户端中引入大量新功能时故意造成的。根据难度的定义，如果分支成为区块链的最长版本，那么它就是成功的。

[0314]FPGA：现场可编程门阵列(场 ProgRamming Gate ArRay)是一种处理芯片，可以在制造后配置自定义功能。可以把它想象成一块可以写指令的空白硅板。由于 FPGA 可以批量生产并在制造后配置，制造商从规模经济中受益，使其比 ASIC 芯片更便宜。然而，它们通常要慢得多。

[0315]自由市场：除了科技巨头接受加密货币和试验区块链外，这项技术在初创企业手中也在不断发展，形成了一个蓬勃发展的区块链市场。天使榜上有一长串区块链初创公司，利用这项技术的企业类型很多，从 SETL 等金融科技(金融科技)初创公司到麻省理工学院初创公司 Enigma，以及 Slock.it 等将区块链技术带入联网汽车、家庭和共享经济的公司。

[0316]FreiCoin：一种基于经济学家西尔维奥・格塞尔(Silvio Gessell)概述的无通胀原则的加密货币。

[0317]无摩擦：就支付系统而言，当交易成本为零或交易限制为零时，系统就是“无功能的”(FHctionless)。

[0318]已满节点：它实现了所有比特币协议，不需要信任任何外部服务来验证交易。它能够下载和验证整个区块链。所有完整节点都实现相同的点对点消息传递协议来交换事务和块，但这不是必需的。完整节点可以使用任何协议并从任何源接收和验证数据。但是，最高的安全性是通过能够尽可能快地与尽可能多的节点通信来实现的。

G。

[0319]燃气：基本网络成本单位。仅由 Ether 支付 FBR 费用(从 PoC-4 开始)，可根据需要自由转换为 Gas。天然气不存在于内部以太计算引擎之外；其价格由交易设定，矿商可以自由忽略天然气价格过低的交易。

[0320]Genesis 区块链中的第一个区块。

[0321]千兆哈希数/秒：给定秒内可能的哈希尝试次数，以数十亿哈希(数千兆哈希)为单位。

[0322]GPU：图形处理单元。一块硅芯片专门设计了 fbr 渲染数百万个现代多边形所需的复杂数学计算。电脑游戏图形学。它们还非常适合于加密货币挖掘所需的加密计算。

[0323]图表间隙：有时，市场价值图上的趋势线会出现缺口。这些差距表明，一种商品的价值出现了明显的下跌或上涨，但这并不一定是因为交易而发生的。这可能是闭市、分析师的统计调整或有关大宗商品的强劲消息的结果。有三种类型的间隙：**[0324]1.。**突破鸿沟(Breakaway Gap)。这些都出现在强劲上涨或下跌趋势的开始，代表着非常大的交易量。

[0325]2.。失控的盖普。这些都发生在上升或下降的趋势中，代表着这一趋势的快速瞬间加剧。

[0326]3.。耗尽差距。这发生在上升趋势或下降趋势接近尾声的时候，并倾向于表明相反方向的小趋势。

H。

[0327]减半：比特币的供应量有限，这使得它们成为一种稀缺的数字商品。比特币的总发行量为 2100 万枚。每个区块产生的比特币数量每四年减少 50%。这就是所谓的“减半”。最后的减半将发生在公元 2140 年。

[0328]硬叉：一些人使用硬叉一词来强调，改变比特币协议需要绝大多数人同意，否则经济中一些引人注目的部分将继续沿用原有的区块链，遵循旧规则。

[0329]硬件钱包：一种比特币钱包，用于在硬件设备上离线存储用户的比特币。

[0330]哈希：一种采用可变数据量并产生较短的固定长度输出的数学过程。散列函数有两个重要特征。首先，通过查看输出很难计算出原始输入是什么。其次，即使更改输入的最小部分，也会产生完全不同的输出。

[0331]要进行散列，请执行以下操作：来计算某些数据的散列函数。如果没有明确提到散列函数，它是由上下文定义的函数。例如，“TO HAVE A TRaNSACTION‘’意味着计算事务的二进制表示的 Hash256。

[0332]Hashl60：使用 RIPEMD-160 散列的 SHA-256 用于生成地址，因为它的散列比 SHA-256 小(20 字节比 32 字节)，但仍在内部使用 SHA-256 FBR 安全性。核心比特币中的 BTCHashl60()。BitcoinQt 中的 Hashl60()。它在脚本中也可以作为 op_HASH160 使用。

[0333]散列，散列 256：当不谈到任意 HAS 函数时，Hash 指的是两轮 SHA-256。也就是说，您应该计算数据的 SHA-256 散列，然后计算该散列的另一个 SHA-256 散列。它用于块头散列、事务散列、创建事务的 Merkle 树或计算地址的校验和。在核心比特币中称为 BTCHash2560()，在 BitcoinQT 中称为 Hash()。它也可以在脚本中作为 op_HASH256 使用。**[0334]散列**函数：散列函数接受任意输入，例如整数字符串(键)，并输出预先指定长度的值(散列)。比特币使用加密散列函数来保护网络安全。

[0335]哈希率：比特币挖掘者在给定时间段(通常为一秒)内可以执行的哈希数。

[0336]散列类型(散列类型)：附加到事务输入中的事务签名的单个字节，描述应如何对事务进行散列以验证该签名。影响输出的类型有三种：All(默认)、Single、None 和一个影响输入的可选修改器 ANYONECANPAY(可以与前三个中的任意一个组合)。ALL 要求对所有输出进行散列(因此，所有输出都是带符号的)。SINGLE 清除除索引与输入相同的输出脚本之外的所有输出脚本。没有清除所有输出，因此允许随意更改它们。ANYONECANPAY 删除除当前输入之外的所有输入(允许任何人独立投稿)。实际的行为比这个概述更微妙，您应该检查实际的源代码以获得更多注释。

[0337]头肩图案：当两个较小的价值波动位于中间一个较大的波动时，市场价值图表上就形成了头肩图案。有两种类型的头部和肩部图案，如上图所示。一种是传统的头部和肩膀，如果你看一个人的半身像，就会看到“右侧朝上”。形成头部和肩膀的波动代表着投资者为了测试当前的趋势而买入和卖出。常规的头肩模式代表了从“牛市”(上升趋势)到“看跌”(下降趋势)的逆转，而倒置的头肩模式则相反，从熊市到牛市。由于这些特点，头肩图案被列为“反转”类型。

[0338]高度：请参见块高度。

[0339]热钱包：一种可以主动连接到互联网的比特币钱包。这些是 FBR“每天”使用的交易，永远不应该持有大量比特币，因为它们的连通性降低了它们的安全性。

[0340]HTML：首字母缩写 FBR“‘HyperText Markup Language(超文本标记语言)”，即编写网页所使用的语言。

[0341]HTTP：“超文本传输协议”的首字母缩写，这是万维网的底层协议 FBR。**[0342]混合**钱包：这是一个加密货币存储和维护系统，是软件钱包(存储在您的家庭计算机上)和 Web 钱包(存储在第三方服务器上)的组合。你的大部分数字货币账户信息都存储在钱包主机的服务器上-除了 FBR 一个重要的细节。您的私钥(唯一标识您的代码)仅存储在您自己的设备上。当您进行交易时，您的私钥在前往 Exchange 服务器的途中被加密，因此他们永远不会知道您的私钥是什么。这是一个令人印象深刻的安全功能，但访问您的私钥还包括一个密码-再说一次-只有您知道。如果您丢失或忘记该密码，可能会拒绝访问您的帐户，并且您可能会永远失去帐户余额。

我。

[0343]工业区块链：保护手表和其他可穿戴设备的交易功能。

[0344]通货膨胀：当货币的价值随着时间的推移而下降时，会导致 FBR 商品的价格上涨。其结果是购买力下降。影响包括减少动力。囤积金钱，更有动力在商品价格仍然较低的情况下迅速消费。

[0345]输入：比特币交易中表示比特币支付来源的部分。通常情况下，这将是一个比特币地址，除非交易是世代交易，这意味着比特币是新开采的(参见 Coinbase)。

[0346]知识产权：FBR 区块链的一个使用案例是保护目前受制于互联网的数字资产和知识产权(IP)。这是智能合同发挥作用的另一个领域，特别是在电影和音乐等数字多媒体文件方面。从理论上讲，艺术家、制片厂和内容提供商认为区块链可以解决盗版问题。这种知识产权保护也可以扩展到使用受版权保护的代码和软件，或者像分享 Netflix 密码或从谷歌上抓取没有标记为 FBR 重用的图像这样琐碎而普通的事情。

[0347]接口系统和方法，两台或更多台计算机使用它们都能理解的公共语言在诸如因特网的网络上相互交谈。

[0348]发卡人：我们公开承认，当我们谈论加密货币时，我们使用这一术语作为一种便利。对于传统货币，发行者将是美国财政部的 FBR 美国纸币和硬币，例如 FBR。从技术上讲，数字货币硬币不是发行的，它们是通过采矿过程创造的。没有中央银行，没有政府决定何时出现新的加密货币：当投资者挖掘数据块时，它是“铸造”的。比特币实际上没有一个所有者，也没有公司董事会做出决定；它的所有投资者都拥有比特币的既得利益和份额。因此，当我们使用术语“发行人”时，我们指的是某种加密货币的投资者；我们是在概念上而不是字面上使用它。

[0349]起点：FBR 区块链的应用是无限的。有一些学校使用区块链来记录和验证学生凭据。德勤(Deloitte)等公司正在讨论使用区块链 FBR 征税。国会代表已经听取了区块链简报。就连美国邮政服务(USPS)也发布了一份关于可能在其运营中采用区块链的报告。区块链还处于相对的初级阶段，但十年后，你不知道你会在哪里找到它。

K。

[0350]密钥：可以指 ECDSA 公钥或私钥，或 AES 对称加密密钥。协议本身不使用 AES(仅用于加密 ECDSA 密钥和其他敏感数据)，因此通常单词 Key 表示 ECDSA 密钥。当谈到密钥时，人们通常指的是私钥，因为公钥总是可以从私钥派生出来的。请参见私钥和公钥。

[0351]密钥池：一些创建新私钥的钱包应用程序随机保留一个未使用的预生成密钥池(默认情况下，BitcoinQT 保留 100 个密钥)。当需要新的密钥时，FBR 更改地址或新的支付请求，应用程序提供池中最旧的密钥，并用新的密钥替换它。该池的目的是确保最近使用的密钥始终备份在外部存储上。如果没有密钥池，您可以创建一个新密钥，收到其地址的付款，然后在备份此密钥之前关闭硬盘。密钥池可以保证该密钥已经备份了几天。

在使用之前。确定性钱包不使用密钥池，因为它们需要备份单个密钥。

[0352]KiLohash/秒：给定秒内可能的散列尝试次数，以数千个散列为单位。**[0353]木本**重力井：这是一种挖掘难度很大的重新调整算法，它是 2013 年为替代币 Megaco in 创建的。这口井允许在每个区块进行困难的重新调整，而不是每个 2016 个区块 FBR 比特币。这样做是为了回应人们对多池采矿计划的担忧。

[0354]KYC：了解你的客户/客户规则迫使金融机构审查与他们做生意的人，确保他们是合法的。

我。

[0355]洗衣房：比特币也被称为"混合服务"，它们将来自不同用户的资金组合在一起并重新分配，通过混合它们的"污点"，使得追踪比特币的原始来源变得非常困难。

[0356]分类帐：一种仅附加的记录存储，其中的记录是不可变的，并且可能包含比财务记录更多的一般信息。

[0357]所有事项分类帐：区块链可以解决物联网功能正常运行的六个障碍：弹性、健壮、实时、响应、完全开放、可再生、可编辑、创收和可靠。

[0358]杠杆作用：在外汇交易中，杠杆将账户中的实际资金乘以给定的系数，使你能够进行能够带来丰厚利润的交易。通过给予交易员杠杆，交易交易所实际上是借钱给他们，希望它能赚回比借出的佣金更多的钱。杠杆也被称为保证金要求。

[0359]自由保护区：总部设在哥斯达黎加的集中式数字货币支付处理器。在被发现犯有洗钱罪后，该公司被美国政府关闭。

[0360]轻量级客户端：与全节点相比，轻量级节点不存储整个区块链，因此不能完全验证任何事务。轻量级节点有两种：一种是完全信任外部服务来确定钱包余额和交易有效性的节点(例如：block chain.infb)；另一种是实现简化支付验证(SPV)的应用。SPV 客户端不需要信任任何特定服务，但比完整节点更容易受到 51%的攻击。请参阅：简化付款验证。

[0361]Litecoin：一种基于解密工作证明的替代币。阅读莱特温新闻，了解更多信息。

[0362]流动性：轻松买卖资产的能力，交易之间的定价大致相同。相当大的买家和卖家群体是重要的 FBR 流动性。缺乏流动性的市场的结果是价格波动，无法轻松确定资产的价值。

[0363]流动性互换：作为加密货币交易所的一种金融工具，流动性掉期是投资者向他人提供贷款进行交易的合约，以换取 FBR 的固定回报。

[0364]LLL：类 Lisp 的低级语言，一种人类可写的语言，使用 FBR 编写简单的合同和通用低级语言工具包 FBR 反编译为。

[0365]锁定时间(锁定时间)：事务中的 32 位字段，表示事务生效的块高度或 UNIX 时间戳。零表示交易。选项在任何块中都有效。小于 500000000 的数字被解释为块号(11000 年后将达到限制)，否则为时间戳。

[0366]彩票被许多州定义为奖品、机会和对价。

M。

[0367]MAC 媒体访问控制。

[0368]主链：区块链中节点认为最困难的部分(请参阅难度)。所有节点存储包括孤儿在内的所有有效块，并在接收到另一个块时重新计算总难度。如果新到达的一个或多个块没有扩展现有的主链，而是从先前的某个块创建了另一个主链，则称为重构化。

[0369]主网：主要的比特币网络及其区块链。该术语主要用于与 Testnet 进行比较。

[0370]追加保证金通知：追加保证金要求的行为。当交易所认为交易员没有足够的资金来支付杠杆交易头寸时，就会发出追加保证金通知。

[0371]融资融券：用借来的钱购买的资产或证券的交易。交易员通常会贡献一笔初始金额，然后将这笔金额用作其债务的抵押品。

[0372]市场秩序：以当时的市价执行的买入或卖出指令。

[0373]市场秩序：对交易所的指示，要求其按现行市场价格买卖资产。在比特币交易所，如果你只是想立即买卖比特币，你就会下市场订单，而不是持有它们，直到触发既定的市场条件，试图获利。

[0374]mBTC：千分之一比特币(0.001 比特币)。

[0375]兆哈希数/秒：给定秒内可能的哈希尝试次数，以百万哈希(数千 KiLohash)为单位。

[0376]Mempool：术语 FBR 是节点存储的未确认事务的集合，直到它们到期或包含在主链中。当重组发生时，孤立块中的事务要么变为无效(如果已经包含在主链中)，要么移到未确认事务池中。默认情况下，bitcoind 节点在 24 小时后丢弃未经确认的事务。

[0377]合并矿业：这允许矿工同时在多个区块链上工作，从而提高了被挖掘的两种货币的散列率(从而提高了安全性)。例如，Namecoin 已经实现了与比特币的合并挖掘。

[0378]Merkle Tree：Merkle 树是一种抽象数据结构，它将数据项的列表组织在散列树中(就像在 Git、MercURial 或 ZFS 中一样)。在比特币中，Merkle 树仅用于组织块内的事务(块标题只包含树的一个散列)，因此满节点可以修剪全部耗尽的事务以节省磁盘空间。如果向 SPV 客户端提供了所有中间散列的列表，则 SPV 客户端仅存储块标头并验证事务。

[0379]消息：通过自主对象的确定性操作或事务的加密安全签名在两个帐户之间传递的数据(作为一组字节)和值(指定为以太。

[0380]留言电话：将信息从一个账户传递到另一个账户的行为。如果目标帐户与非空的 EVM 代码相关联，则 VM 将以所述对象的状态和所操作的消息启动。如果消息发送者是自治对象，则调用将传递从 VM 操作返回的所有数据。

[0381]小额交易：支付少量 FBR 来购买资产或服务，主要是在线支付。小额交易在传统支付系统下很难进行，因为涉及的佣金很高。以 FBR 为例，用你的信用卡阅读一篇在线文章很难花 2 美分。

[0382]矿工：参与任何加密货币网络执行工作证明的计算机。这通常是为了获得大宗奖励。

[0383]采矿：通过使用计算硬件解决密码问题来生成新比特币的行为。**[0384]挖掘**算法：加密货币用来对比特币网络中的交易进行签名的算法，将区块添加到区块链上。

[0385]采矿合同：一种投资比特币挖掘硬件的方法，允许任何人在约定的时间内出租预先指定数量的散列能力。矿业服务负责硬件维护、托管和电力成本，使其成为更简单的 FBR 投资者。**[0386]矿池：**一群矿工决定将他们的计算能力结合起来进行 FBR 挖掘。这使得奖励可以在池中的参与者之间更一致地分配。

[0387]铸币厂：Satoshi 通过将比特币的发行与创建新的区块分类账联系起来分发铸币，将铸币的权力交到了同行网络的所有人手中。

[0388]铸币帽：当加密货币矿工处理交易数据块时，他们会因此产生新的硬币。加密货币是一个年轻的行业，其发行人希望有足够的硬币流通，以满足新投资者的加入。这些新硬币的数学设计是以稳定的速度生产，因此货币的价值也将保持相对稳定(就像在任何其他大宗商品市场一样，会有波动，但不会像商品供应极其有限的情况下那样疯狂)。然而，随着时间的推移，硬币创造的数学也被设计为结束，以避免市场过饱和和货币贬值。简单地说，这意味着当大多数加密货币达到一个被称为铸币上限的预定数量时，它们最终将停止被创造。一旦最后一枚硬币被创造出来，就不会再有了。在大多数情况下，FBR 在几年内都不会达到上限-这是设计好的，所以新的投资者将被允许在未来一段时间加入 FBR。大多数加密货币都有铸币上限：然而，也有少数像 PeerCoin 这样的一-on。

[0389]铸币：在证明赌注硬币时奖励使用者的过程。新硬币被铸造，作为 FBR 在一块内验证交易的奖励。

[0390]混合：为了增加个人历史的私密性而与他人交换硬币的过程。有时它与洗钱联系在一起，但严格地说，它与洗钱是正交的。在传统银行业中，银行通过向所有第三方隐藏交易来保护客*户*隐私。在比特币中，任何商家都可以对一个人的整个支付历史进行统计分析，并确定一个人拥有多少比特币，比如 FBR。同时。仍然可以在每个商家的级别上实施 KYC(了解您的客户)规则，混合允许在商家之间提供关于个人历史的单独信息。最重要的 FBR 混合使用案例包括：1)收到一份月薪，然后花在小额交易中(“CAFB 在你只付 4 美元时就能看到数千美元”)；2)一次性付款，揭示出许多小额私人支出之间的联系(“汽车经销商看到你有多么沉迷于咖啡”)。在这两种情况下，你的雇主、咖啡馆和汽车经销商可能会遵守 KYC/AML 法律，并报告你的身份和转账金额，但他们都不需要知道对方的情况。在拿到工资后混合比特币，然后在支付大笔款项之前混合比特币，就解决了这个隐私问题。

[0391]混合服务：将您的比特币与其他比特币混合的服务，将输入和输出与您发送的比特币不同的比特币送回。混合服务(也被称为 TUmbler)保护了你的隐私，因为它阻止人们追踪特定的比特币到你。它还有可能被用于 FBR 洗钱。

[0392]移动钱包：这是一种运行“移动客户端”的钱包，人们可以在手机和平板电脑上使用比特币钱包，并在移动中进行支付。

[0393]货币政策：另一个突破是保留软件中编程的价值。

[0394]洗钱：通过将犯罪活动中赚取的利润转化为看起来合法的资产，试图“清理”这些钱的行为。

[0395]M-of-N 多重签名交易：需要 N 个公钥(M 小于或等于 N)时可以使用 M 个签名进行的事务。只包含一个 OP_CHECKMULTSIG 操作码且 N 为 3、2 或 1 的多重签名事务被视为标准事务。

[0396]Mt.。Gox：最早的比特币交易所之一，一度也是最受欢迎的。MT.。自那以后，Gox 进入了破产管理程序。该交易所总部设在日本，由杰德·麦凯勒(Jed McCaleb)于 2010 年创立。

[0397]多重签名：多重签名地址允许多方使用公钥部分播种地址。当有人想要花掉一些比特币时，除了他们自己之外，他们还需要这些人中的一些人签署他们的交易。当人们创建地址时，所需的签名数量在开始时就已达成一致。使用多重签名地址的服务具有更强的防盗能力。

n

[0398]Namecoin：一种替代币，旨在提供传统域名系统(DNS)的替代方案。用户可以通过域名支付来注册.bit 域，可以通过代理服务器访问。

[0399]网络效应：增值当一种商品或服务的使用变得更加广泛时，它的价值就会增加。**[0400]NFC：**近场通信是“近场通信”的缩写，是一种低功耗、短距离的无线通信方法。这可以用于构建 RFID 系统，也是非接触式智能卡(牡蛎卡)和支付系统(PayPass)的用途。最近在 Apple Pay 应用程序中实现了这一功能。

[0401]节点：使用客户端连接到比特币网络的计算机，该客户端将交易中继给其他人(请参阅客户端)。

[0402]随机数：在对事务块进行散列时用作输入的随机数据字符串。现时值用于尝试生成符合比特币难度设置的数字参数的摘要。每次散列尝试将使用不同的随机数，这意味着在尝试散列每个事务块时会生成数十亿个随机数。

[0403]非标交易：任何非标准的有效交易。默认情况下，BitcoinQT 节点不会中继或挖掘非标准事务(而是在 testnet 上中继和挖掘)。但是，如果任何人将此类事务放入块中，则所有节点都会接受该事务。在实践中，这意味着不寻常的交易需要更多时间才能纳入区块链。如果某种非标准事务变得有用和流行，它可能会被命名为标准，并被用户(喜欢)采用。请参阅标准事务处理。

[0404]Noob 陷阱：“noob”是“新血液”的缩写，有时也表达为“newb”或“newbie”。它适用于任何在这种情况下是给定社区一的新手，投资于数字货币。大多数另类货币投资者都是好人，愿意向那些刚接触这个游戏的人伸出援手，提供建议。然而，也有一些人认为新手很容易被盯上，这些不择手段的投资者经常利用操纵市场的方法来利用那些可能还不知道更好的人。幸运的是，对这些方法进行一些明智的研究，可以帮助新投资者保护自己，使自己免于落入市场操纵陷阱。为了更好地理解数字货币世界中存在的新手陷阱的类型，请参见术语熊市陷阱、牛市陷阱以及泵送和倾倒。

[0405]诺瓦科因：尽管这种类型的加密货币还没有接近该行业大型参与者的价值或整体投资者数量，但 Novaco in 仍在前五名中占有一席之地；考虑到它是在 2013 年 2 月推出的，这还不错。Novaco in 使用 SCRYPT 挖掘算法，并通过联合证明-oSwork 和 prooSof-Start 方法进行挖掘。

O。

[0406]对象：同义词 FBR 自治对象。

[0407]区块链外交易：信任方之间发生在区块链之外的价值交换。之所以会出现这些情况，是因为它们速度更快，并且不会阻止区块链。

[0408]账外币种：梅杰铸造的一种货币，在分类账上使用。这方面的一个例子是使用分布式分类账来管理国家货币。

[0409]脱机存储：此概念与您的加密货币的存储方式相关。如果你的货币是在线的--在一台打开的或可通过云计算访问的电脑上的活动驱动器--那就意味着其他电脑用户也可以使用它。有时，这种访问是在您不知情的情况下进行的。这可能会导致黑客攻击和盗窃，因为加密货币--从设计上讲，一与任何一个人都没有直接联系。因此，尽可能多地保持您唯一的货币信息离线是很重要的；最好是这样做，除非该货币正在 FBR 交易中直接使用。让你的投资信息离线的最好方法有两种，一种是将它存储在一个外部驱动器上，当它不需要的时候，它可以从你的电脑上断开连接；或者把它打印出来，然后存储在一个纸质钱包里。如果您决定利用加密货币交易所提供的钱包服务，您应该首先问他们一个问题。应该是关于离线信息存储，因为数字货币盗窃通常是无法追踪和不可逆转的。

[0410]分类帐上币种：一种铸造在分类账上并在分类账上使用的货币。这方面的一个例子是加密货币。比特币。

[0411]操作码：脚本操作的 8 位代码。从 0x01 到 0x4B(十进制 75)的代码被解释为要推送到解释器堆栈上的数据长度(操作码后面是数据字节)。其他代码要么做一些有趣的事情，要么被禁用并导致交易验证失败，或者什么都不做(保留 FBR 将来使用)。请参见脚本。

[0412]开放网络企业：随着智能合约变得越来越复杂，并与其他合约进行互操作，这就促成了这一点。

[0413]开源：共享一款计算机软件的源代码，允许任何人分发和修改它的做法。

[0414]孤儿街区：该块不是有效区块链的一部分，而是被丢弃的分叉的一部分。

[0415]场外交易所：交易员之间直接进行交易，而不是依靠中央交易所进行调解的交易所。

[0416]输出：目的地址是比特币交易的 FBR。单个事务可以有多个输出 FBR。

[0417]硬币拥有者：以太选择了这一点作为它的经济设置。涟漪和明星选择了社交网络。

[0418]计算能力的拥有者：智史选择了这个经济模式。这就要求这些矿工要想参与奖励制度，就必须消耗网络之外的一种资源，即电力。

P。

[0419]纸质钱包：包含一个或多个公开比特币地址及其对应私钥的打印页。通常用于安全地存储比特币，而不是使用软件钱包或网络钱包，因为软件钱包可能会被破坏，网络钱包可能会被黑客入侵或干脆消失。一种有用的冷比特币存储形式。

[0420]参与者：可以访问分类帐的参与者：读取记录或将记录添加到。

[0421]Pay-to-Script 哈希：一种脚本和地址类型，允许使用任意复杂脚本的紧凑散列将比特币发送到该脚本。这使得付款人支付的交易费要少得多，而不需要等待很长时间 FBR 非标准交易才能纳入区块链。则在兑换资金时必须由收款人提供与散列匹配的实际脚本。P2SH 地址采用 Base58 校验编码，就像普通公钥一样，并以数字“3”开头。

[0422]对等点：共同承担责任的行为者，负责维护分类账的身份和完整性。

[0423]对等币：第一种与工作证明一起实施“风险证明”的加密货币。

[0424]P2P：点对点。高度互联网络中至少两方之间发生的分散交互。一种替代“轴辐式”安排的系统，在这种安排下，交易中的所有参与者都通过单个中介点进行交易。

[0425]锦旗图案：当投资者想要测试一种商品价值的当前趋势时，这种模式就会出现在市场价值图表上。在测试期间进行的买卖--通常持续一到三次。

Week 一形成的波动可以被汇聚的对角线所包围，形成一个“旗帜”形状。这些旗型在上升趋势(“熊市”)和下降趋势(“牛市”)期间都可能出现。因为它们并不意味着当前的趋势将会逆转，所以旗型被认为是一种“同质化”的模式类型。一旦格局形成，趋势将继续朝着之前的方向发展。

[0426]许可分类帐：授权分类帐是一种分类帐，参与者必须具有访问分类帐的权限。授权的分类帐可能有一个或多个所有者，当添加新记录时，通过有限的协商过程检查分类帐的完整性。这是由受信任的参与者一政府部门或银行执行的，例如一，它使得维护共享记录比未经许可的分类账使用的协商一致过程简单得多。被许可的区块链提供了高度可验证的数据集，因为协商一致过程创建了一个数字签名，所有各方都可以看到。许可的分类帐通常比未经许可的分类帐快。

[0427]电话到电话转接：这是一种移动应用程序功能，允许将信息从一部智能手机即时传输到另一部智能手机。如果两个移动设备用户想要交换数据，并且都在他们的电话上安装并激活了此功能，他们只需将他们的设备放在彼此很近的地方就可以进行传输。这些有时也被称为“触摸传输”。

[0428]平台交换：这是一个数字货币交易所，限制了它们在投资者之间进行的交易中发挥的作用。大多数交易所都是为了促进这些交易，并使它们更容易进行。该交易所将对买入和卖出订单进行分类，然后将符合相关订单标准的投资者进行匹配。他们的算法经过精心设计，使得交易对双方都是安全和公平的。不过，除此之外，交易所并不扮演任何“中间人”或调停角色。这与交易所形成鲜明对比，交易所将以第三方托管交易资金，或者在推进交易之前与两家投资者讨论交易细节。

[0429]池：一群采矿客户，他们共同开采一个区块，然后在他们之间平分报酬。随着难度的增加，矿池是增加成功开采区块的概率的有效方法。

[0430]PPCoin：也就是点对点硬币或点对点硬币。一种将赌注证明机制与工作证明相结合的替代币。根据桑尼•金和斯科特•纳达尔撰写的一篇论文。

[0431]开采前：在一种加密货币的创始人开采硬币之前，该硬币还没有被宣布，细节也被公布给了其他可能想要开采硬币的人。预采是一种常用的预采技术，尽管并不是所有预采的硬币都是预采的(见 ScamCoin)。

[0432]价格泡沫：一种经济周期，其中证券或资产的价格将不可持续地飙升，然后在抛售发生时崩盘。这通常是由投机引起的，从比特币过去的价格中可以看出这一点。如果故意这样做，这就是所谓的“抽水倾倒”。

[0433]Primecoin：由 Sunny King 开发的 Primecoin 使用工作证明系统来计算素数。

[0434]私有货币：一种由私人或公司发行的货币，通常以未投保的资产为抵押。

[0435]私钥(PrivKey)：由用户保密的字母数字字符串，用于在使用公钥进行散列时对数字通信进行签名。就比特币而言，此字符串是专为使用公钥而设计的私钥。公钥是比特币地址(参见比特币地址)。

[0436]流程节点：在芯片制造过程中产生的以纳米为单位的晶体管尺寸。流程节点越小，效率越高。

[0437]活动证明：把工作证明和赌注证明结合起来。

[0438]爆炸证明：这是一种“烧录”一种工作证明加密货币以获得另一种加密货币的方法。这是一种将一种加密货币从另一种加密货币上“自举”的形式，通过将硬币发送到一个可验证的不可消费地址来实现。

[0439]能力证明：要求矿工将相当数量的硬盘分配给采矿。

[0440]存在证明：一项通过区块链提供的服务，允许任何人匿名和安全地存储存在的证明，FBR 任何他们选择的在线文档。这使人们能够证明文档在某个时间点存在，并证明他们对文档的所有权，而不必担心证据会从他们手中夺走。

[0441]立桩证明：工作证明的另一种选择，即你在一种货币中的现有股份(你持有的该货币的金额)被用来计算你可以开采的该货币的金额。

[0442]存储证明：需要挖掘者在分布式云中分配和共享磁盘空间。

[0443]工作证明：一种将挖掘能力与计算能力捆绑在一起的系统。必须对块进行散列，这本身就是一个简单的计算过程，但是在散列过程中添加了一个额外的变量使其更加困难。当成功地对块进行散列时，散列必须花费一些时间和计算工作量。因此，哈希块被认为是工作的证据。

[0444]消费者：生产产品的客户。

[0445]协议演变：区块链是互联网协议自然演变的结果。《连线》讲述了 1974 年最初的 TCP/IP 互联网网络协议和 Tim Berner-Lee 的超文本传输协议(HTTP)是如何以与区块链相同的方式演变的，正在演变为下一代互联网，将多种协议捆绑在一起形成未来框架的基础，并“从头看着互联网的诞生”。

[0446]PSP：支付服务提供商。PSP 为希望接受在线支付的 FBR 商家提供支付处理服务。

[0447]P2SH：请参见付费脚本哈希。

[0448]公钥(PubKey)：一种公知的字母数字字符串，它与另一个私人持有的字符串进行散列以签署数字通信。在比特币的情况下，公钥是比特币地址。

[0449]利用大张旗鼓的宣传和经常误导性的陈述，抬高廉价生产或收购的金融资产的价值。公开性导致其他人获得资产，迫使其。

价值。当价值足够高时，犯罪者出售他们的资产，变现并淹没市场，导致价值暴跌。

问。

[0450]左右为难：区块链从一开始就受到争议的困扰，从中本聪(Satoshi Nakamoto)正在进行的传奇故事到这项技术与比特币的千丝万缕的联系以及随之而来的所有合法性。区块链使非法加密货币交易具有不可追踪性，甚至被用来掩盖 CryptoLocker 等臭名昭著的勒索软件骗局。随着这项技术在更多的行业和用例中被采用，责任和后果问题需要解决。已经开始看到这样的努力了。区块链联盟是一个非营利性组织，由比特币倡导团体创建，旨在充当一种“公私结合的平台，帮助打击区块链上的犯罪活动。”成员包括主要的加密货币参与者，如 Coinbase、麻省理工学院媒体实验室的数字货币倡议和区块链组织本身。**[0451]量**化宽松：中央银行采取的一种货币政策形式。

[0452]二维码：包含表示数据序列的单色图案的二维图形块。二维码是为摄像头(包括手机中的摄像头)扫描而设计的，经常被用来对比特币地址进行编码。

R。

[0453]参考实施：比特币 Qt(或位编码)是使用最多的全节点实现，因此它被认为是其他实现的参考。如果替代实现与 BitcoinQT 不兼容，则它可能会被破坏，也就是说，它将不会看到与运行 BitcoinQT 的网络的其余部分相同的主链。

[0454]中继交易：相互连接的比特币节点在尽力的基础上相互中继新的交易，以便将它们发送到挖掘节点。有些事务可能不是由所有节点中继的。例如非标准交易，或者没有最低费用的交易。比特币信息协议并不是发送交易的唯一方式。也可以直接寄给矿工，自己挖矿，或者直接寄给收款人，让他们转送或挖矿。

[0455]汇款：汇款通常在国际上作为付款或礼物寄出的一笔钱。

[0456]REO 昭，REOI^ANIZATION：当主链中的一个或多个块变为孤立时节点中的事件。通常，新收到的数据块是对现有主链的扩展。有时(每周 4-6 次)几乎同时产生几个相同高度的块，并且 FBR 在短时间内，一些节点可能会将一个块视为主链的顶端，最终将被更难的块所取代。孤立块中的每个事务要么变为无效(如果已包含在主链块中)，要么变为未经确认并移至内存池。如果出现重大错误或 51%的攻击，重组可能涉及重组多个块。

[0457]复制分类帐：具有一个主(授权)数据副本和多个从(非授权)副本的分类帐。

[0458]反转图形模式：这是一种在市场价值图表上形成的模式，你可以在许多数字货币兑换网站上看到。反转模式表明，一直处于上升趋势的市场(即所谓的“牛市”)将逆转方向，开始向下行进，或者变成“熊市”--反之亦然。当反转图形模式出现时，它表明投资者一直在测试当前的趋势，FBR 出于这样或那样的原因，他们认为这种趋势不可行或不可持续-因此市场改变了方向。

[0459]奖励：矿工可以在新区块中认领的新生成比特币的数量。该区块的第一笔交易允许矿商要求目前允许的奖励，以及从该区块所有交易的所有交易费中收取交易费。奖励大约每 4 年减半 210000 个街区。截至 2014 年 7 月 27 日，奖励为 25BTC(第一次减半发生在 2012 年 12 月)。出于安全原因，奖励不能在 100 个街区之前花掉，这些街区是在现有图书的基础上建造的。

[0460]波纹：可用于转移任何货币(包括用户创建的临时货币)的支付网络。该网络由当局运营的支付节点和网关组成。支付使用一系列逻辑单元，网络基于信任关系。

[0461]圆底：有时也被称为“碟底”，这是一个术语 FBR，你可以在交易所网站的市值图表上看到这种模式。圆底形态被认为是一种“反转”形态，也就是说，随着时间的推移，它代表了一个下跌趋势或“熊市”市场向上升的“牛市”市场的过渡。上图左侧缓缓向下倾斜的线条跟踪市场，当它最终找到底部或最低市值时，然后-通常同样温和和缓慢-趋势向上。这是一种非常长期的模式，通常需要几个月到几年的时间才能完全形成。

%s。

[0462]智史：目前可用的比特币的最小细分(0.00000001 比特币)。

[0463]中本聪：比特币协议的最初发明者使用的名字，他于 2010 年底退出了该项目。

[0464]假币：一种替代币，其唯一目的是让发起人赚钱。Scamcoins 经常使用抽水和倾倒技术，并一起进行预开采。

[0465]脚本：一种紧凑的图灵不完全编程语言，用于事务输入和输出。脚本由类似 Forth 的堆栈机器解释：每个操作都操作堆栈上的数据。大多数脚本遵循标准模式，并对照前一事务输出中提供的公钥验证事务输入中提供的数字签名。签名和公钥都是使用脚本提供的。脚本可能包含复杂的条件，但永远不能更改正在传输的金额。金额存储在事务输出的单独字段中。

[0466]scriptPubKey：Bitcoind FBR 中的原始名称是事务输出脚本。通常，输出脚本包含公钥(或其散列：请参见地址)，这些公钥只允许相应私钥的所有者兑换输出中的比特币。

[0467]scriptSig：事务输入脚本的原始名称(以位字符表示)。通常，输入脚本包含签名以证明先前交易发送的比特币的所有权。

[0468]加密：SHA-256 的替代工作证明系统，设计为对 CPU 和 GPU 矿工特别友好，而对 ASIC 矿工几乎没有优势。**[0469]密钥：**加密钱包中使用私钥或加密密钥。比特币协议在任何地方都不使用加密，因此密钥通常意味着使用 FBR 签名交易的私钥。

[0470]顺序：事务输入中的 32 位无符号整数，用于将事务的旧版本替换为新版本。仅在锁定时间不为零时使用。直到序列号为 OxFFFFFFFF，交易才被视为有效。

[0471]种子：确定性钱包中使用的私钥。

[0472]自动执行合同：也称为“智能合同”，这些协议在不需要 FBR 人工干预的情况下促进或执行合同义务。

[0473]卖单：当投资者接触交易所，打算出售部分或全部加密货币投资时，就会发生这种情况。有时卖出指令简单而直截了当(“只要以你能找到的最好的价格卖出我所拥有的东西”)，或者投资者可以设定在卖出之前必须满足的标准。这可能包括价格、时间范围、出售所持股份的百分比等。大多数交易所都有可以填写的卖出订单表格，但如果投资者有特定的问题或担忧，他们可以在激活订单之前直接与交易所代表交谈。

[0474]国家环保总局：欧洲单一支付区。欧盟内部的一项支付一体化协议，旨在使不同银行和国家之间更容易用欧元转移资金。

[0475]SHA-256：作为 FBR 比特币工作证明系统基础的加密函数。

[0476]侧链：这些都是理论上独立的区块链，与比特币区块链“双向挂钩”。它们可以有自己的独特功能，并可以将比特币发送到它们和从它们接收比特币。

[0477]签名：通过将私钥和公钥散列在一起来证明比特币交易来自特定地址而生成的数字摘要。

[0478]丝绸之路：一个地下在线市场，通常使用 FBR 非法购买，通常使用比特币等加密货币。2013 年 10 月初，在所有者罗斯 • 乌布里奇特(Ross Ulbricht)被捕后，丝绸之路被联邦调查局关闭。乌布利赫特后来被判洗钱和毒品分销躺椅罪名成立。

[0479]简化支付验证(SPV)：一种无需存储整个区块链(仅区块标头)和不信任任何外部服务来验证事务的方案。每个事务必须存在于 Merkle 树中直到根的所有父哈希和兄弟哈希中。SPV 客户端信任最困难的块头链，并可以验证事务是否确实属于某个块头。由于 SPV 不会验证所有交易，51%的攻击不仅可能导致重复花费(就像满节点一样)，而且还会用无处可见的比特币进行完全无效的支付。但是这种攻击呢，是非常昂贵的，而且可能比有问题的产品更贵。BitcoinJ 库在功能上实现了 SPV。(参见 SPV)。

[0480]切片馈送：SliceFeeds 是 Coin PURching 的免费社交网络，它将所有交易员、矿工和爱好者的联系人和加密货币信息集中在一个地方，从而消除了麻烦。成员可以将对话、笔记、谣言、提示、链接和视频剪切到其他社区成员以供其关注。它的网络分为三个简单易用的部分：网络页面一目了然地显示统计数据；切片页面在更新发生时显示；以及个人资料页面允许成员定制他们自己的网络中的个人网络。会员还可以将他们对社区的独特贡献货币化；例如，博客作者可以为他们的独家内容提供订阅(当然是以数字货币支付)，商家也可以通过 SliceFeed 为他们的公司和产品做广告。

[0481]切片：切片是会员在 Coin PURching 提供的社交媒体网络 SliceFeed 上提供的内容。这些片段可以由对话、笔记、谣言、提示、链接和视频组成，供 FBR 其他社区成员关注、评级和查看。

[0482]智能合同：智能合同是以计算机语言而不是法律语言记录条款的合同。智能合约可以由诸如合适的分布式分类帐系统的计算系统自动执行。

[0483]软叉：有时，软分叉指的是软件行为的一个重要变化，而不是硬分叉(例如，改变挖掘费政策)。请参见硬叉和叉子。

[0484]源代码：开放源码软件，包括管理比特币规则、FBR、移动和所有权的协议，以及保护和验证比特币交易的密码系统。

[0485]投机者：投机比特币或任何其他形式资产价格的个人。旨在通过以不同的价格买卖来赚取利润。

[0486]垃圾邮件：不正确的对等消息(如发送无效事务)可被视为拒绝服务攻击。有效的交易金额很小和/或采矿费很低的交易被一些人称为灰尘(Dust)。协议本身没有定义哪些事务不值得中继或挖掘。这是每个单独节点的决定。如果节点希望接受剩余的区块，区块链中的任何有效交易都必须被节点接受，因此交易审查只意味着增加确认延迟。个人收款人也可能将某些地址列入黑名单(拒绝接受来自某些地址的付款)，但这太容易使用混合解决方案。

[0487]消耗产量：事务输出只能使用一次：当另一个有效事务从其自己的输入引用此输出时。当另一个事务试图花费相同的输出时，它将被已经看到第一个事务的节点拒绝。区块链作为一种 ProoSof-Work 方案，允许每个节点就哪一笔交易确实是第一笔交易达成一致。当整个事务的所有输出都用完时，就认为整个事务已用完。

[0488]拆分：区块链的分裂。请参见叉子。

[0489]SPV：简化付款验证。比特币协议的一项功能，使节点无需下载完整的区块链即可验证支付。相反，他们只需要下载块头。

[0490]陈旧：当一个比特币块被成功散列后，任何其他试图散列它的人都可能会停止，因为它现在已经“过时”了。他们只是在重复别人已经做过的工作，没有报酬。TERN 还用于矿池中，用来描述已经完成的散列作业的份额。

[0491]陈旧区块：一个已经解决的区块，因此不能为矿工提供任何奖励，FBR 在它上面做进一步的工作。

[0492]标准交易：有些事务被认为是标准事务，这意味着它们由大多数节点进行中继和挖掘。更复杂的事务可能有漏洞或导致网络上的 DoS 攻击，因此它们被认为是非标准的，不会被大多数节点中继或挖掘。标准和非标准交易都是有效的，一旦被纳入区块链，将被所有节点识别。标准事务处理包括：1)发送到公钥，2)发送到地址，3)发送到 P2SH 地址，4)发送到 N 为 3 或更小的 M-OSN 多重签名事务。

[0493]止损单：这是站着说“让我离开这里！”股票或大宗商品(如加密货币)的投资者用来卖出的订单，嗯.。止住他们的损失。或者至少最小化它们。投资者通常在买入的那一刻就建立止损指令。这是一个卖单，指定货币应该卖出的价格。例如，如果你以每股 100 美元的价格买入某家公司的股票，你可能会决定以 60 美元的价格发出止损单。只要股价保持在这个数字以上，一切都很好一，除非你亲自联系交易所，否则什么都不会发生。然而，一旦价格达到 60 美元，你的全部或部分货币(无论你指定的)将以你的止损指令价格出售。不同的交易所对待这一点是不同的；一些交易所立即抛售，一些交易所等待，看看这是否只是市场上的一个短暂的“小插曲”；如果价格跌破你的止损限制，你将获得后者的 FBR 你的股票。

[0494]存储状态：在帐户的关联 EVM 代码运行期间维护的特定于给定帐户的信息。

T。

[0495]污点：当两个地址都持有特定比特币时，对这两个地址关联程度的分析。污点分析可以用来确定 FBR 比特币从已知 FBR 被盗硬币的地址移动到当前地址需要多少步骤。

[0496]目标：一个 256 位的数字，它将上限 FBR 设置为有效的块头散列。目标越低，找到有效人选的难度就越高。最大(最简单)目标是 0X00000000FF00000000000000000000000000000000000000000000000000。难度和目标每隔 2016 个区块调整一次(约。2 周)以保持块之间的间隔接近 10 分钟。

[0497]TCP/IP: 首字母缩写代表 FBR“传输控制协议(TRansfer Control ProtocorV)、互联网协议(Intemet Protocol)”，是互联网使用的连接协议。

[0498]太哈希数/秒：给定秒内可能的哈希尝试次数，以万亿哈希(千兆哈希)为单位。

[0499]测试网：另一种比特币区块链，纯粹用于 FBR 测试目的。

[0500]测试 3：带有另一个创世模块的最新版本的 Testnet。

[0501]时间戳：证明某一数据在某一时间点存在的证据。对于比特币来说，这是交易何时发生的加密证据。

[0502]无令牌分类帐：无代币分类账是指不需要本币操作的分布式分类账。

[0503]TOR：一种匿名路由协议，供想要在网上隐藏身份的人使用。

[0504]硬币总供应量：对于许多加密货币来说，将会出现的硬币总数是有限制的，比特币的总供应量上限为 2100 万枚。

[0505]交易墙：一般来说，图表上的趋势线(如数字货币交易所提供的趋势线)会随着交易的进行或多或少地沿对角线移动。然而，偶尔会有买入或卖出指令出现，这会让趋势线直接上下移动，形成一条类似于墙的垂直线。这些“墙”代表着人们对购买或出售某种数字货币的兴趣暂时高涨。如果一堵墙是由大额买入订单造成的，它被称为“买入墙”，如果它代表着一笔可观的卖单，它就被称为“卖出墙”。一般说来，这些墙被称为“交易墙”或“出价墙”。一旦订单被填满-r 通常被市场忽视-这堵墙就消失了，对角线趋势线继续。

[0506]交易记录：一条数据，由外部演员签名。它表示消息或新的自治对象。交易记录到区块链的每个区块中。

[0507]交易区块：比特币网络上的交易集合，收集成一个区块，然后可以进行散列并添加到区块链中。

[0508]交易数据库：从纯技术角度来看，区块链是交易数据库。散列、键和节点都构成了一个避开集中式存储的分布式数据库。

[0509]交易费：对通过比特币网络发送的一些交易征收的一小笔费用。交易费奖励给成功散列包含相关交易的块的挖掘器。

[0510]交易录入：事务的一部分，其中包含对前一个事务的输出的引用，以及可以证明该输出所有权的脚本。脚本通常包含签名，因此称为 scriptSig。投入完全消耗了之前的产出。因此，如果只需要支付以前输出的一部分，事务应该包括额外的更改输出，将剩余的部分发送回其所有者(在相同或不同的地址上)。Coinbase 事务只包含一个输入，该输入带有对前一个事务的零引用和替代脚本的任意数据。

[0511]交易产出：输出包含要发送的金额和允许进一步支出的脚本。脚本通常包含公钥(或公钥的地址、散列)和签名验证操作码。只有相应私钥的所有者才能创建将该金额进一步发送给其他人的另一事务。在每笔交易中，产出金额的总和必须等于或小于所有投入金额的总和。请参见更改。

[0512]三角形阵列：一般来说，当投资者买入和卖出以检验当前趋势时，市场价值图表上会形成三角形模式。这些波动的高点和低点可以用直线包围，这些直线定义了测试期间的高点和低点；这些直线形成了一个开放的三角形。有三种类型的三角形图案：

[0513]1.。降三角。当三角形的下线是水平线，而上线从左向右向下倾斜时，就会形成这种情况。下降三角形代表下跌趋势或"熊市"。**[0514]2.**。上升三角。这是下降三角形的反面，底部有一条从左向右向上倾斜的线，顶部有一条水平线。上升的三角形模式预示着即将到来的"牛市"或上升趋势。

[0515]3.。对称三角形。对称三角形之所以突出，是因为构成该三角形的两条线都是倾斜的。这也是一个更难预测的模式，因为它可以继续向上("看涨")或向下("看跌")的方向。

[0516]三底图案：当投资者买入和卖出以测试价值下降趋势时，市场图表上就会形成一个三重底部模式。买入和卖出将会发生，随着时间的推移，这将在图表的趋势线上形成三个截然不同且几乎相等的山谷。一旦第三个谷地形成，上升趋势将超过模式形成过程中形成的山峰或顶部的点。一旦发生这种情况，市场可能会在一段时间内"看涨"，或上升趋势，FBR；因此，三重底部模式被认为是一种"反转"模式，从熊市过渡到牛市。

[0517]三项图案：当投资者买入和卖出以测试价值上升趋势时，市场图表上就会形成一个三重顶模式。买入和卖出将会发生，随着时间的推移，这将在图表的趋势线上形成三个截然不同且几乎相等的峰值。一旦第三个峰值形成，下跌趋势将在形态形成过程中形成的下坡点或谷点处形成。一旦发生这种情况，市场很可能会在一段时间内"看跌"或下跌，即FBR；因此，三重顶形态被认为是一种"反转"形态，从牛市过渡到熊市。

[0518]TX：请参阅交易。

[0519]TXIN：请参阅：事务处理输入。

[0520]TXOUT：请参阅交易输出。

使用。

[0521]无处不在：区块链无处不在；在字母表中，这已经不是什么新闻了。开放源码，区块链的普遍适用的架构，以及它们分发、匿名、保护和保持完美准确的网络交易记录的能力，使这项技术成为既定技术。

[0522]Ubtc：一枚微比特币(0.000001 比特币)。

[0523]未确认交易：不包括在任何块中的事务。也称为"O-确认"交易。未确认的事务由节点中继，并留在内存池中。未经确认的事务会一直留在池中，直到节点决定将其丢弃、在区块链中找到它、或将其包含在区块链中、或将其包含在区块链本身中(如果它是挖掘器)。请参阅确认号。

[0524]唯一节点列表：其他区块链，如 Ripple 和 Stella，依赖于社交网络 FBR 共识，并可能推荐新的参与者(即新的节点)来生成唯一的模式列表。

[0525]未经许可的分类帐：未经许可的账簿，如比特币，实际上没有单一所有者一，它们不能被拥有。未经许可的分类帐的目的是允许任何人向分类帐提供数据，并允许所有拥有分类帐的人拥有相同的副本。这会产生阻力，这意味着没有参与者可以阻止将交易添加到分类帐中。参与者通过就分类账的状态达成共识来维护分类账的完整性。

[0526]UTXO 设置：未使用的事务输出的集合。通常用于讨论如何优化尚未花费的事务输出的不断增长的索引。索引对于有效验证新创建的事务非常重要。即使新事务的速率保持不变，查找和验证未花费的输出所需的时间也会增加。可能的技术解决方案包括更高效的索引算法和更完善的硬件。例如，BitcoinQT 只保存与用户键匹配的输出的索引，并在验证其他事务时扫描整个区块链。一位网络钱包服务的开发者提到，他们维护着 UTXO 的整个索引，当区块链本身只有GB 的时候，它的大小在 100 GB 左右。一些人寻求社会方法来解决这个问题。例如，通过拒绝中继或挖掘被认为是粉尘的交易(包含的产出小于开采/中继它们所需的交易费)。

V

[0527]虚荣地址：具有所需模式(如名称)的比特币地址。

[0528]瓦林特：这个术语可能会引起混淆，因为它意味着不同比特币实现中的不同格式。请参见压缩大小。

[0529]货币流通速度：货币流通速度是衡量收到的钱再次花掉的速度的一个指标。对于比特币，我们用"比特币销毁天数"来衡量其速度，这可以表明人们是在囤积比特币还是在消费比特币。

[0530]风险投资家：可以指提供初始资金的个人或组织，但无法获得公共资金的 FBR 初创企业。这笔钱被称为"种子基金"，通常用于交换初创企业的 FBR 股权。

[0531]核查：区块链在没有验证的情况下不会作为分类账工作。这在很大程度上取决于矿工，他们的区块创建软件在将交易捆绑成区块时，会验证交易的散列。在加密货币和银行场景中，支付验证也是至关重要的。这一验证通过分布式网络中的节点通信进行，在发送比特币交易之前，将其与每个节点的区块链数据进行交叉检查。

[0532]维珍比特币：购买比特币作为奖励，FBR 挖掘一个区块。这些钱还没有花在任何地方。

[0533]波动性：对一段时间内价格变动的测量 FBR 是一种交易的金融资产(包括比特币)。

W。

[0534]钱包：一种存储比特币以备日后使用的方法。钱包持有与比特币地址相关联的私钥。区块链是与这些地址关联的比特币金额的记录。

[0535]钱包：就像纸币和硬币钱包一样，这里是存放数字货币的地方。加密货币钱包有四种类型：

[0536]1.。软件钱包。这些程序是您加载到台式机或笔记本电脑上的程序。

[0537]2.。移动钱包：这些应用程序以您在智能手机或平板电脑上安装的应用程序的形式出现。它们通常包括二维码扫描和电话到电话转账 FBR On-The-Go 交易。

[0538]3.。网络钱包：这些数据通常通过交换获得，并通过云计算存储在第三方服务器上。它们可以被任何计算设备访问。**[0539]4.纸质**钱包：你的数字货币可以打印出来，通常是 OR 码一一的形式，这些硬拷贝的加密货币“账单”可以像传统货币一样保存在一个实体钱包里。

[0540]看门狗：区块链发展的速度有多快，并在全球主要市场得到采用，在很大程度上将取决于政府的监督和监管。欧盟(EU)市场监管机构-欧洲证券和市场管理局(ESMA)最近宣布，将更仔细地研究区块链技术。欧盟监管机构是世界管理机构对与分布式分类账相关的金融和技术风险进行仔细检查的一个典型例子。欧盟不会是最后一个在批准使用 FBR 之前对区块链进行长时间、认真研究的政府。

[0541]楔形图案：这是一种你会在市场价值图上看到的“持续”模式；这意味着它们代表了与当前趋势相反的短暂转变，但一旦模式完全形成，趋势往往会继续朝着原来的方向发展。楔形模式可以通过两条对角但不收敛的线来发现，这两条线涵盖了投资者测试当前趋势时出现的上下波动。有三种类型的楔形图案：**[0542]1.**。上升楔形区。这种楔形向上倾斜，因此得名。然而，上升的楔形出现在下跌趋势或“熊市”期间。这是一个短暂的上升趋势，但之后熊市仍在继续。

[0543]2.。坠落的楔子。下落的楔子向下倾斜。它代表的是上升楔形的对立面，因为它表示在“牛市”行情中短暂的向下移动，一旦楔形形成，牛市就会持续下去。

[0544]3.。水平楔形。在图表上，这些似乎或多或少地沿着水平方向移动。就像上升和下降的楔形一样，水平楔形在趋势中显示出短暂的喘息，一旦楔形图案完成，这种趋势将继续下去。

[0545]电汇：通过电子方式把钱从一个人转到另一个人。通常用于从比特币交易所发送和检索法定货币。

X。

[0546]XBT：非正式货币代码 FBR 1 比特币(定义为 100 000 000 Satoshis)。一些人建议使用 FBR 0.01 比特币，以避免与比特币混淆。有传言称，彭博社将 XBT 测试为 FBR 1 比特币，但目前只有 XBTFUND FBR Second-Market 的比特币投资信托基金。参见 BTC。

[0547]XRP：XRP 也被称为 Ripple，是一个建立在区块链基础上的全球支付网络，在国际银行销售。Xrp 本身是昭应用程序可以用来表示平面货币、加密货币、商品或任何其他价值单位的原生货币。涟漪是使用区块链的开放支付协议最古老的例子之一，但也有一长串公司拥有不同的 API、平台和分布式支付网络。德勤(Deloitte)的银行业展望最近发布了一份报告，估计到 2020 年，基于区块链的支付系统可能会与美国自动清算所(ACH)金融交易网络的规模相当。

是

[0548]收益率曲线：收益率曲线是绘制不同期限利率的一种金融方法。为了区块链的目的...。谈论收益率曲线，因为越来越多的银行和金融公司、支付提供商以及国家都在关注和采用区块链。世界各地的公司。都在推动区块链 FBR 转账和支付。此外，菲律宾的立法者多年来一直在推动 FBR 创造一种“e-比索”作为官方的电子招标。区块链正在世界的许多角落扎根，但在实现获得批准和采用的速度和彻底程度方面，将看到广泛的成熟曲线。

Z

[0549]零币：一种旨在使加密货币交易真正匿名的协议。

[0550]零确认交易在比特币的传输得到矿工确认并添加到区块链之前，商家乐于提供产品或服务的交易。它可能会带来重复支出的风险。

[0551]零确认交易：在某些情况下，数据 FBR 加密货币交易的处理可能需要半分钟以上到十分钟以上的任何时间。虽然这对于验证交易是必要的-并防止重复消费等欺诈性活动-但等待时间可能会给参与交易的人带来不便。因此，一些与数字货币打交道的交易所和企业正在提供“零确认”交易，这些交易几乎可以立即得到验证，而无需等待 FBR 挖掘过程来确认数据块。Double Spend 一(双重确认交易)一名硬币持有者将同一种货币用于两笔不同交易的做法一是一种对零确认交易的担忧。由于加密货币没有以任何方式“依附”于消费它的人，当他们的双重支出通过挖掘过程被发现时，他们早就不见了，无法追踪。随着 FBR 零确认交易需求的上升，加密货币行业的企业家们正在寻找立即验证一或拒绝交易的方法，而不必等待 FBR 挖掘发生。与此同时，许多企业收取费用，以抵消零确认交易的财务风险，但还有一些企业拒绝接受这些费用，直到技术跟上。

[0552]Z 系统：IBM 公开承诺在许多方面推进区块链技术，但该公司。

甚至为 IBM Cloud 上的 FBR 开发人员提供区块链即服务(Baas)平台，并在 IBM z Systems 上集成基于区块链的应用程序(通过 Hyperledger 项目创建)。IBM 甚至计划在 Watson Lot 平台上利用区块链与 Watson 相结合，使来自基于 RFID 的位置、条形码扫描事件或设备报告的数据等设备的 FBR 信息能够与 IBM 的区块链一起使用，并与分布式分类账和智能合约同步。这是一个勇敢的基于区块链的新世界。

我们声称：

1. 一种训练人工智能系统的系统 FBR，包括使用一个或多个人类受试者对刺激的反应作为人工智能系统的输入，包括：

一个或多个显示器，该显示器面向人类受试者以向人类受试者呈现刺激，

用于监视人类受试者对刺激的反应的一个或多个检测器，所述检测器至少包括运动检测器，所述检测器提供输出，

分析系统，该分析系统耦合成接收检测器的输出，该分析系统提供对应于人类受试者的反应是阳性还是阴性的输出，以及。

神经网络，其中分析系统的输出提供：

当分析系统的输出为正时，神经网络的正权重 FBR 训练，以及。

当分析系统的输出为负值时，对神经网络进行负权重 FBR 训练。

2. 所述系统 FBR 训练如权利要求 1 所述的人工智能系统，其中所述神经网络训练是强化学习。

3. 所述系统 FBR 训练如权利要求 1 所述的人工智能系统，其中所述显示器是监视器。

4. 根据权利要求 1 所述的训练人工智能系统的系统 FBR，其中所述显示器是虚拟现实显示器。

5. 所述系统 FBR 训练如权利要求 1 所述的人工智能系统，其中所述分析系统监视个人行为。

6. 如权利要求 1 所述的系统，其特征在于，所述系统 FBR 训练人工智能系统，其中所述分析系统监视群体行为。

7. 该系统 FBR 训练权利要求 1 的人工智能系统，其中检测器是运动跟踪系统。

8. 所述系统 FBR 训练如权利要求 1 所述的人工智能系统，其中所述检测器包括面部检测系统。

9. 如权利要求 8 所述的系统，其特征在于，所述系统 FBR 训练人工智能系统，其中所述面部检测系统确定正面和负面面部属性。

10. 所述系统 FBR 训练如权利要求 1 所述的人工智能系统，其中所述检测器还包括声音检测器。

11. 该系统 FBR 训练权利要求 10 的人工智能系统，其中声音检测器是麦克风。

12. 该系统 FBR 训练如权利要求 1 所述的人工智能系统，其中所述检测器是生物测定扫描仪。

13. 该系统 FBR 训练权利要求 1 的人工智能系统，其中该检测器是生理检测器。

14. 根据权利要求 13 所述的系统 FBR 训练人工智能系统，其中所述生理检测器是心率检测器。

(19)美国。

(12)专利申请公开(10)。编号：美国 2018 年/0341861 Al。

Katz et al.　　(43)酒吧。日期　2018 年 11 月 29

(54)用于程序定义状态系统的体系结构、系统和方法。

(71) 申请人：里程碑式的娱乐。
有限责任公司，加利福尼亚州贝弗利山庄
(美国)。

(72) 发明者：兰德尔·M·卡茨，贝弗利山。
加州(美国)；罗伯特·特切克(Robert
Tercek)，好莱坞，加利福尼亚州(美国)。

(21) APPL。编号：16/052,207。

(22) 提交： 2018 年 8 月 1 日。

相关的美国申请数据。

(63)延续 2018 年 2 月 1 日提交的第 15/886,432 号申请。

(60)临时申请第 62/454,423 号，于 2 月 1 日提交。
3、2017 年。

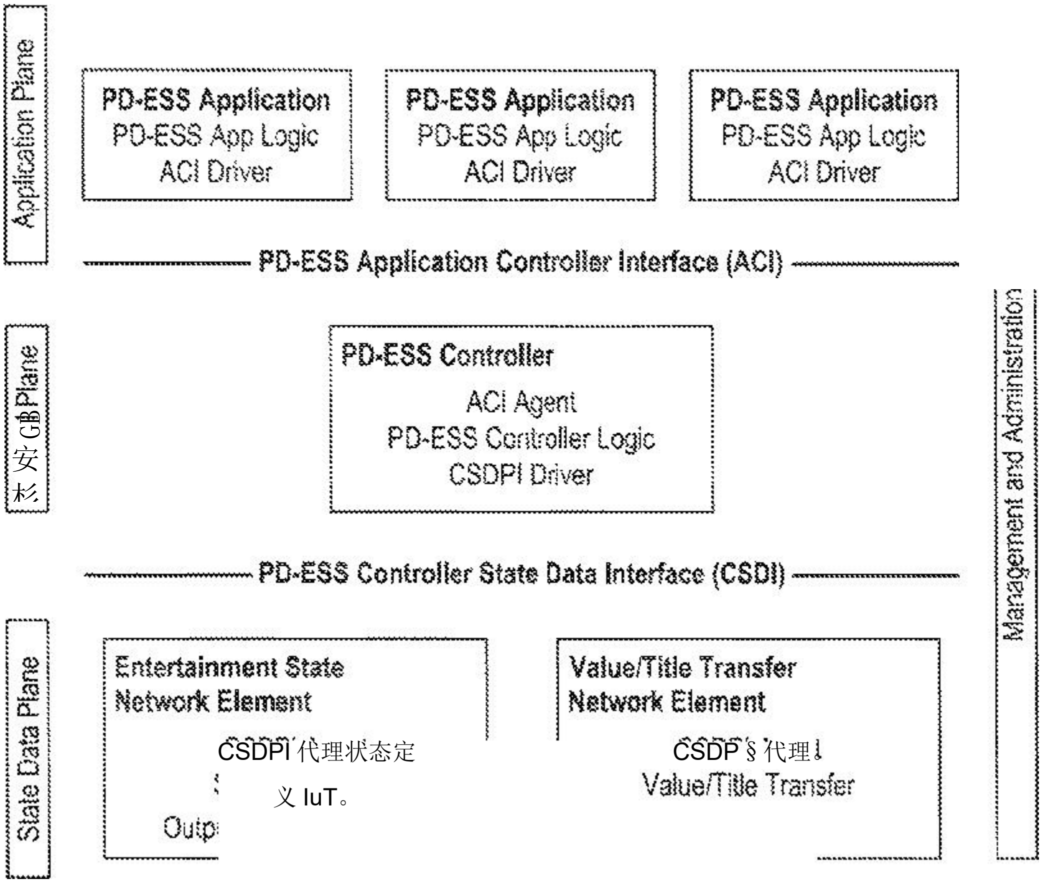
出版物分类。

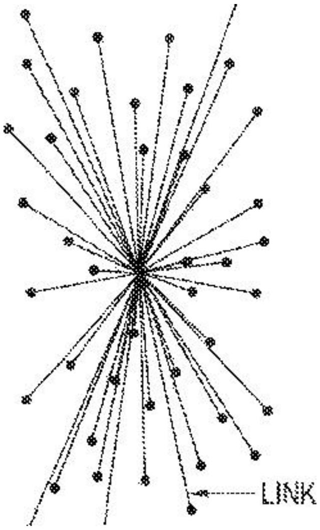
(51) 内部。氯。
G06N 3/08(2006.01)。
G06K 9/00(2006.01)。
G07F17/32(2006.01)。
G06Q 20/06(2006.01)。

(52) 美国 CL。
CPCG06N3/08(2013.01)；G06K 9/00221。
(2013.01)；G06Q 20/065(2013.01)；G07F
17/329(2013.01)。

(57)摘要

一方面，本发明包括娱乐状态系统的系统 FBR 控制。首先，应用平面层适于接收关于娱乐状态系统的操作的指令。优选地，应用平面层耦合到应用平面层接口。第二，控制平面层包括自适应控制单元，例如认知计算单元、人工智能单元或机器学习单元。第三，数据平面层包括输入接口以接收来自一个或多个数据源的数据输入。



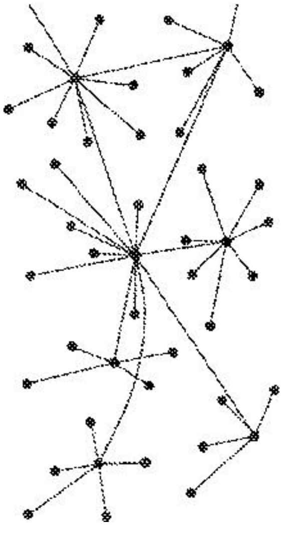


车站。

集中式(A)PnoRartCentRafeed 系统。

插图。1

(现有技术)。



去中心化。

现有技术分散系统。

(PnoRart)。

专利申请公布 2018 年 11 月 29 日美国 2018 年/0341861 年度第 2 页。

PD^ESS AppOeatlon|。 |PD-ESSAppIteatton。 PD-ESS

PD-ESS 应用逻辑 I。 PD-ESS 应用程序日志。 PD~ESSApp 日志。

AQ 驱动程序|。 褊驱动程序。 ACS 驱动程序。

ACI 代理 PD-ESS 控制逻辑 CSDP § 驱动程序 “。

我是说。 J 值/滴定转移。

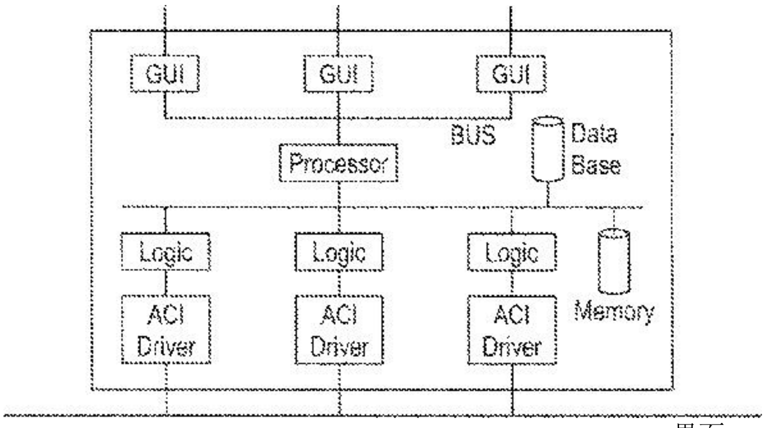
J Netwad<ETEM^NT。

好了！ CSDPI 代理。 CSDPI 代理。

<n J。 ： 统计数据定义。 VAhe/T^e 转接。

：输出输入。

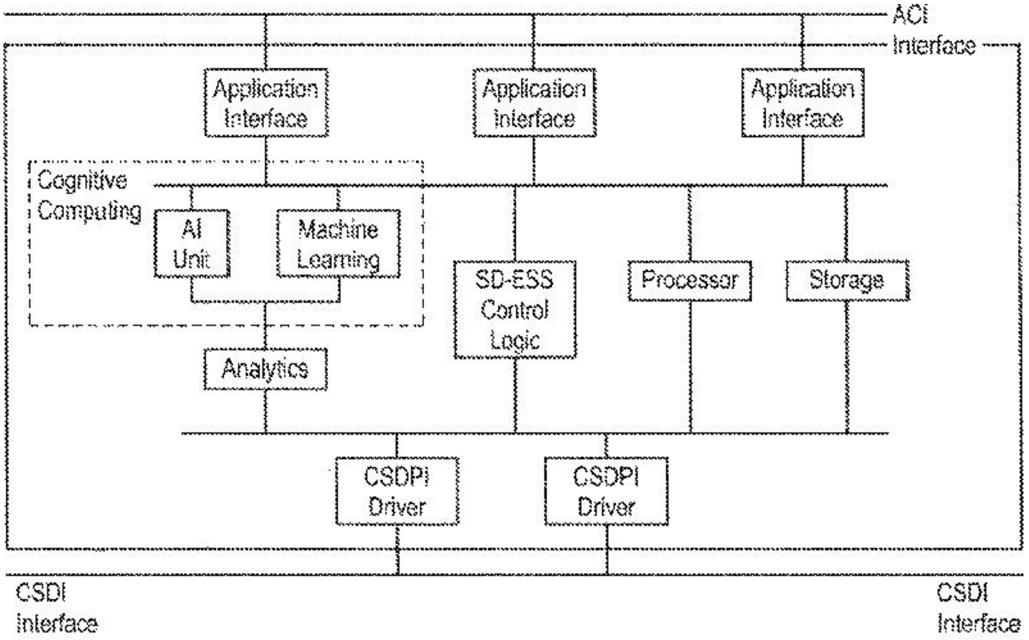
本人：…－_™__“。



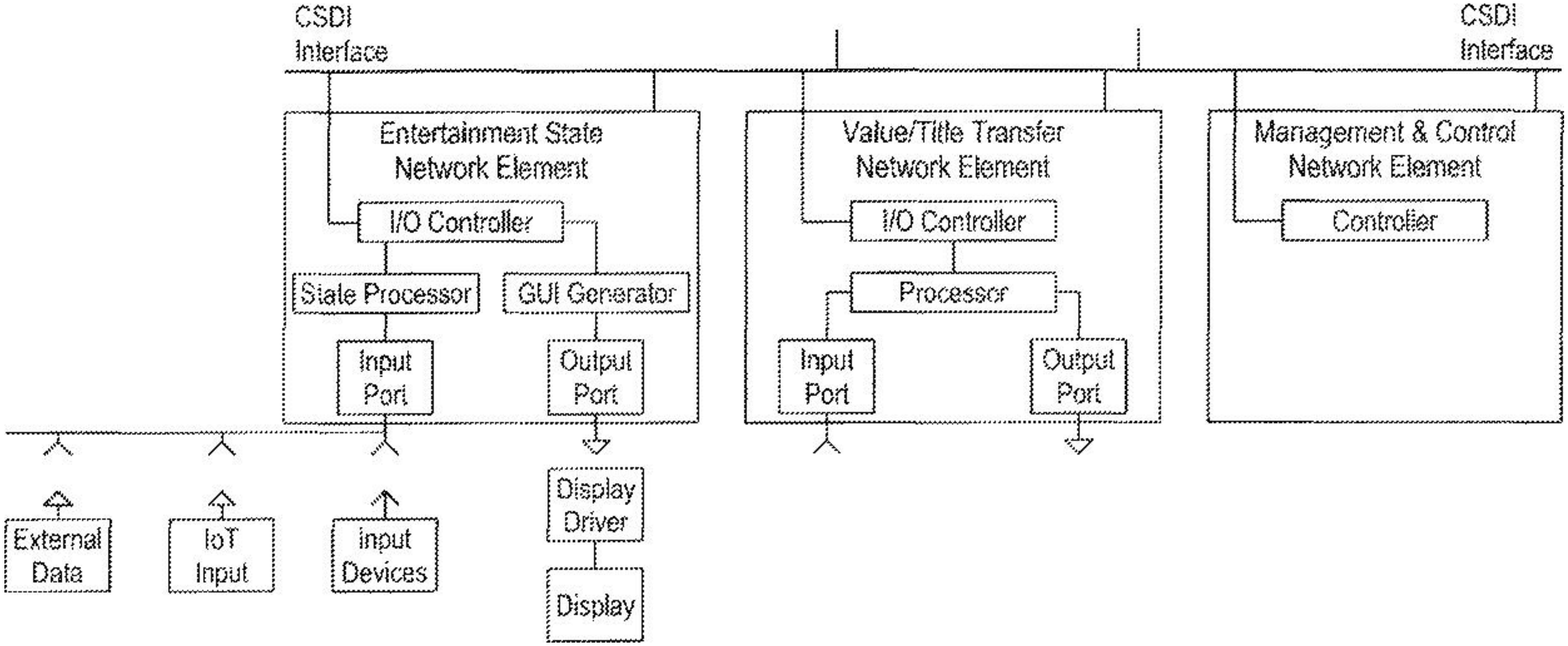
界面。

插图。4

专利申请公布 **2018 年 11 月 29 日美国 2018 年/0341861 年度第 3 页。**



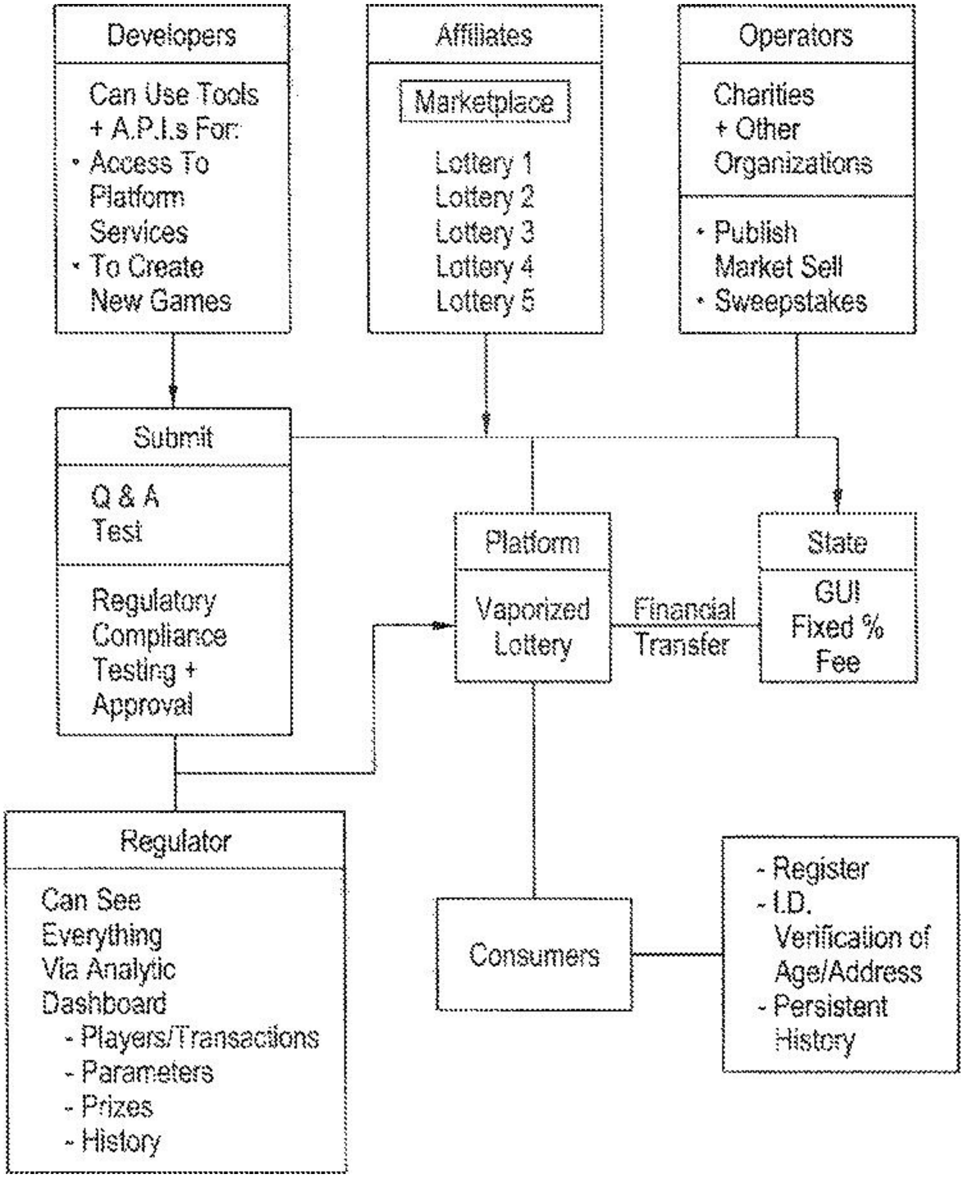
Control Plane Layer Explosion



vbl. 。

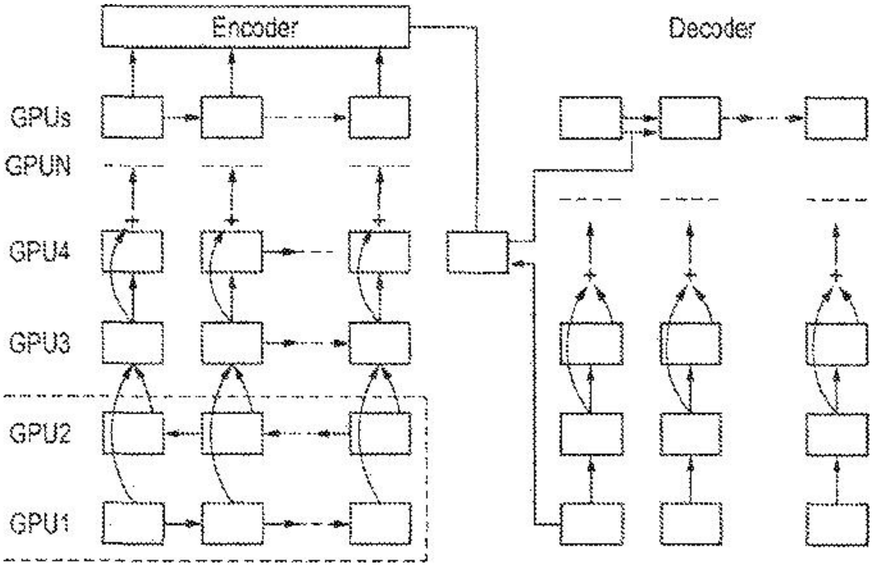
A®段 AXW

bjzJST0a 蕊«s«。



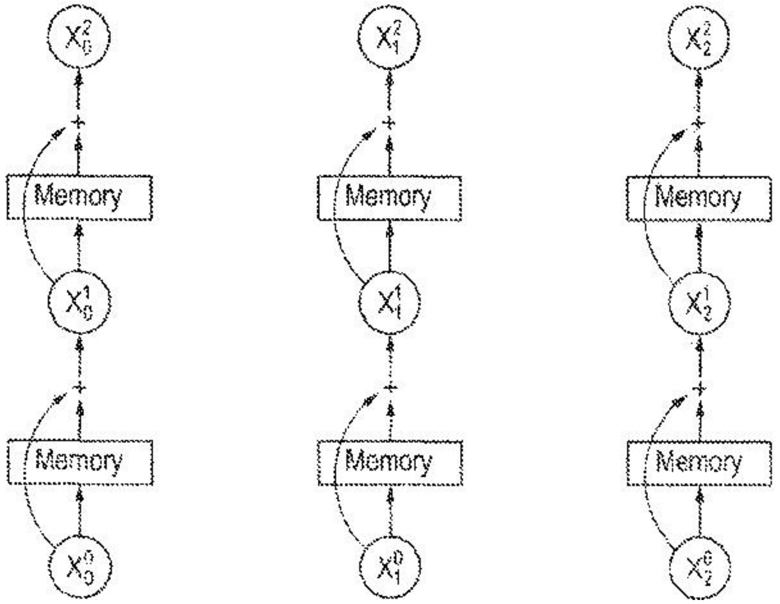
生态系统接口和 hiterconnectiQos。

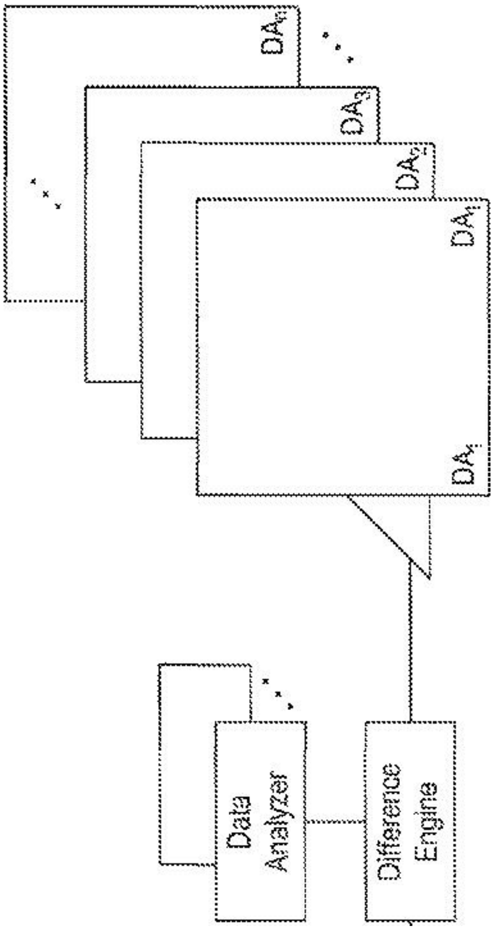
Rlq.。7



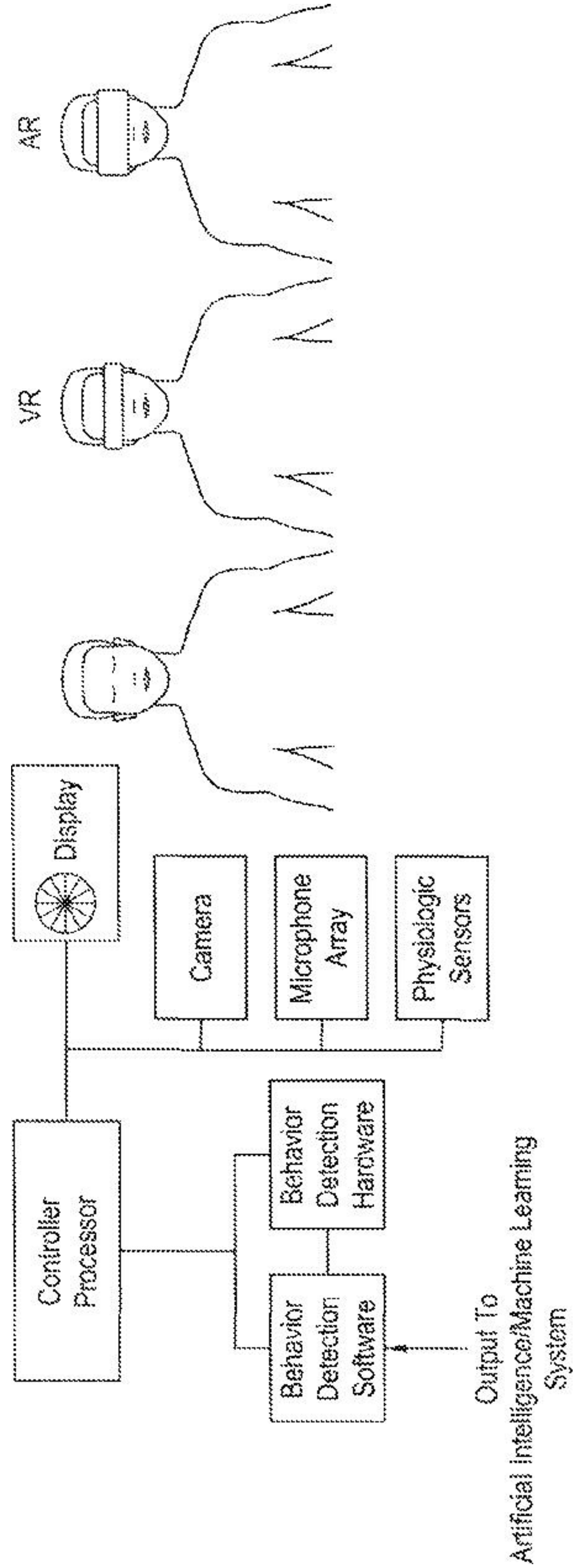
Neural Network Model Architecture

FIG. 8

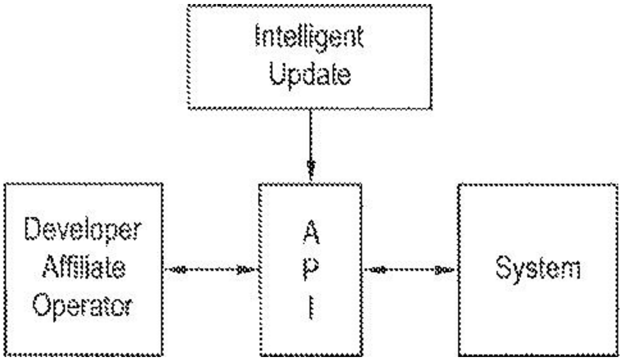



DA_n
DA_3
DA_2
DA_1
DA_1
Data Analyzer
Difference Engine

专利申请公布 2018 年 11 月 29 日美国 2018 年/0341861 年度第 8 页。

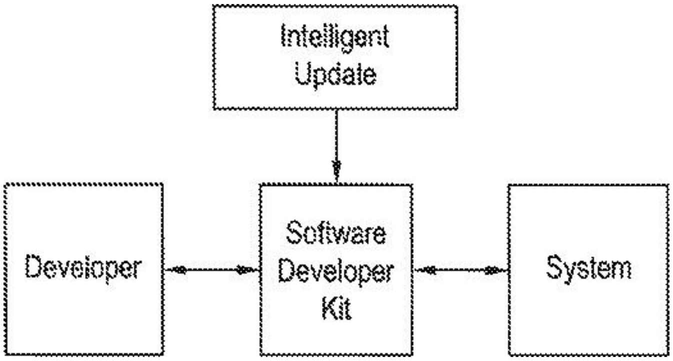

AR
VR
Display
Camera
Microphone Array
Physiologic Sensors
Controller Processor
Behavior Detection Hardware
Behavior Detection Software
Output To Artificial Intelligence/Machine Learning System

M O 七



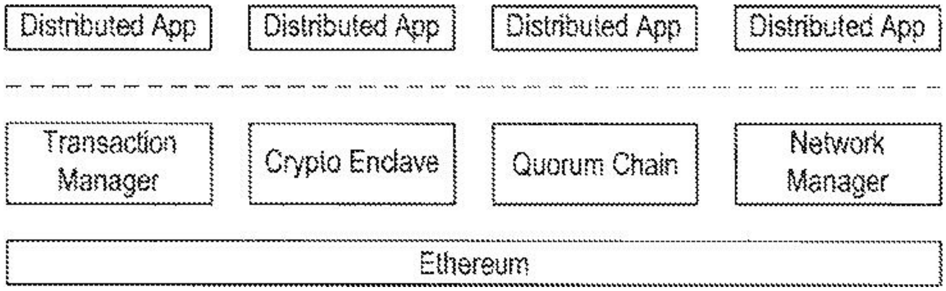
动态系统 d-API。

插图。12



Dynamic Systems d-SDK。

插图。13

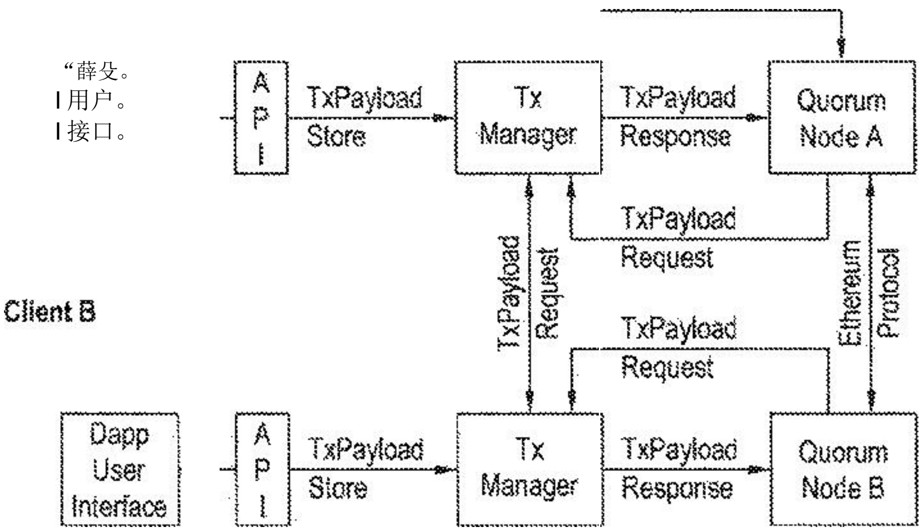


ArehHectURe。

图 14。

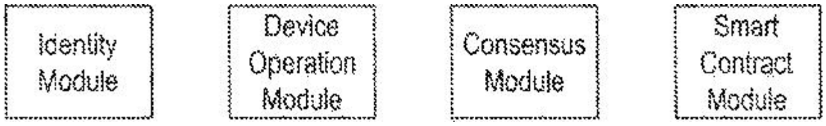
吟诵 A。

“薜殳。
l用户。
l接口。



系统。

插图。15

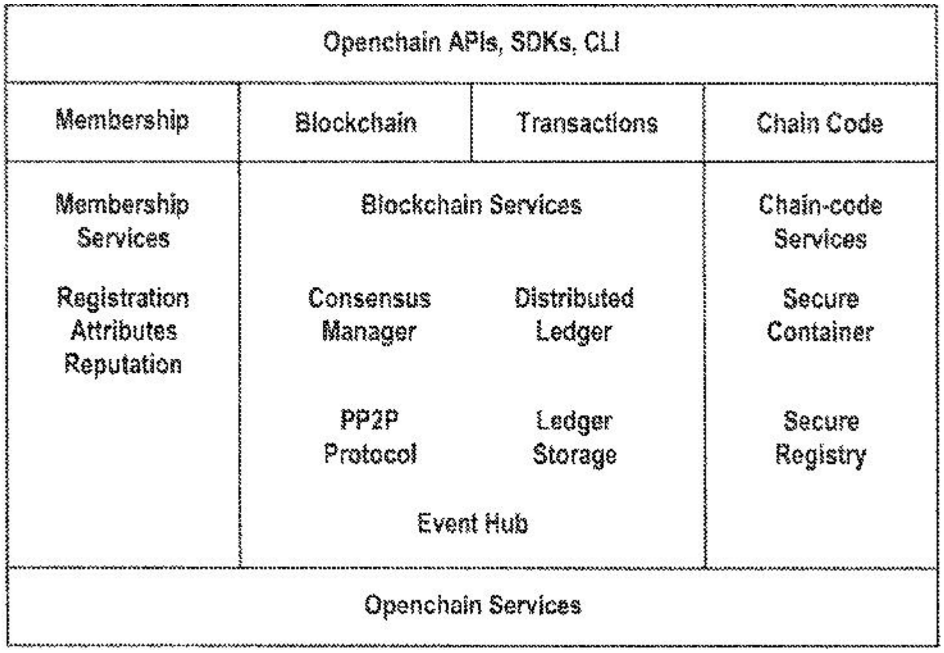


\织物。
|hyp 令独 g 渤 j。

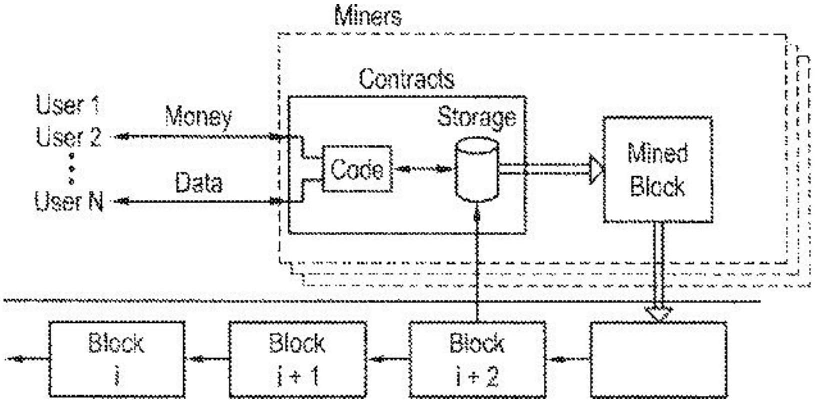
|[云丁丽面]。

Blockcham Platfomi。

插图。16

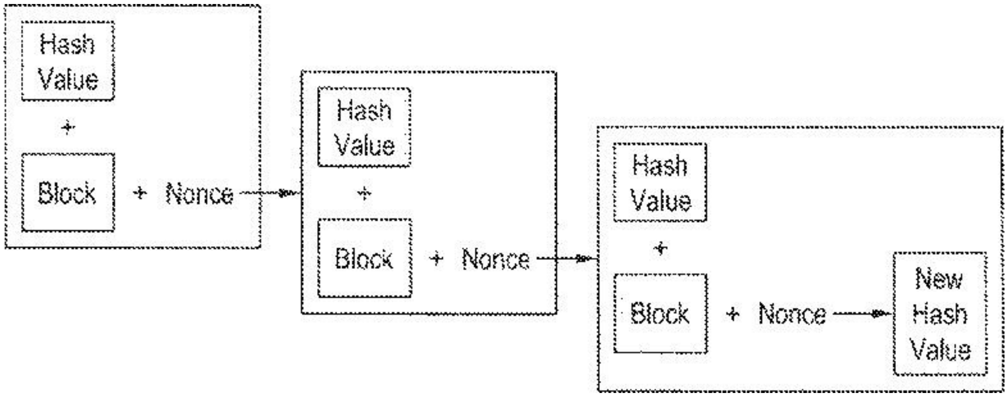


插图。17



具有CoHTR、CTS的Deoentrsfesd CryptooURreney
系统原理图。

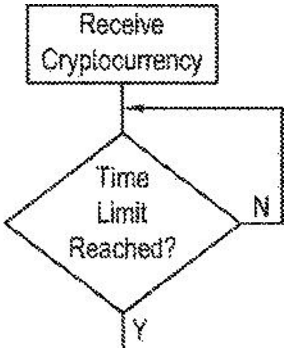
ES 1Q。



顺序 H^sh 值创建梆龄 h 值块加随机数 Hew Hash 值的模式)。

F/A。

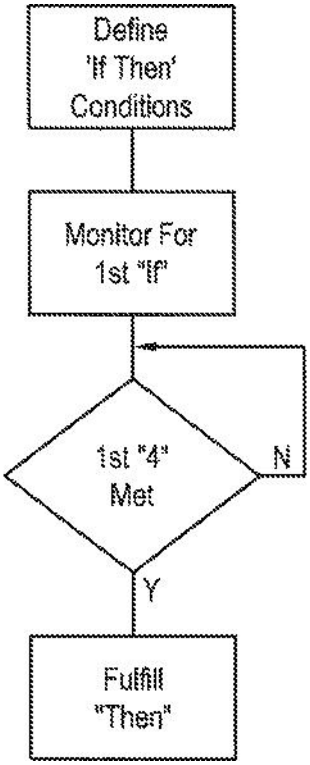
定义条件。



生成。
随机事件。

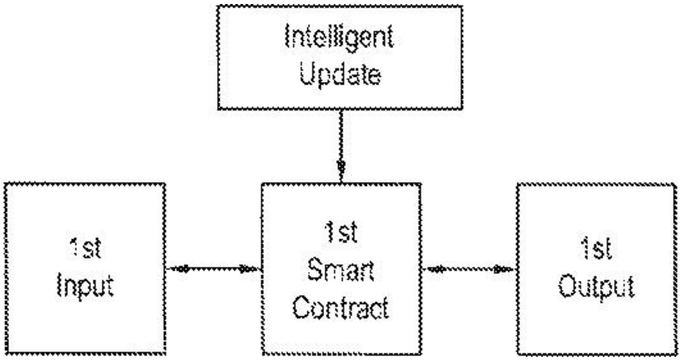
效应。
THTE/VAFEE。
转接。

是否为加。



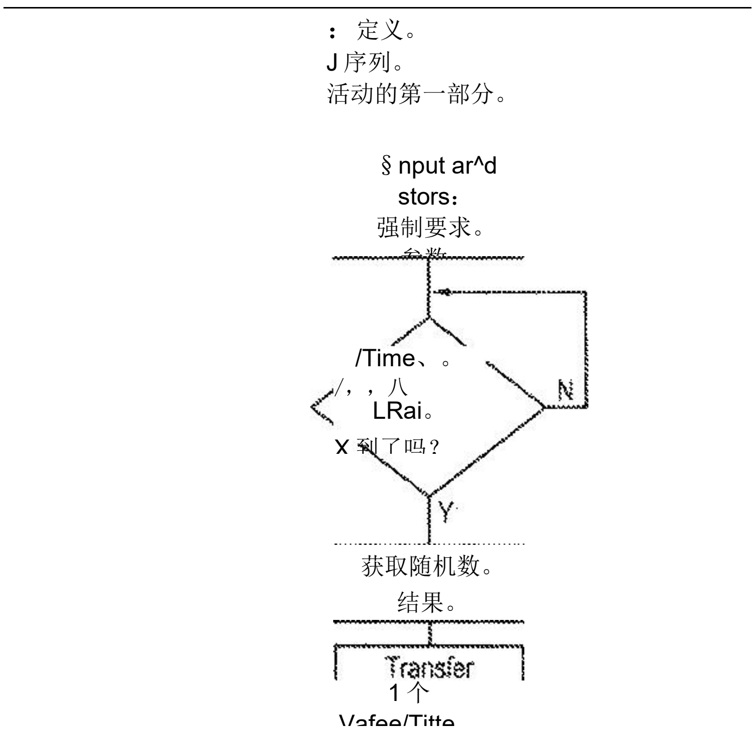
智能契约。

GB



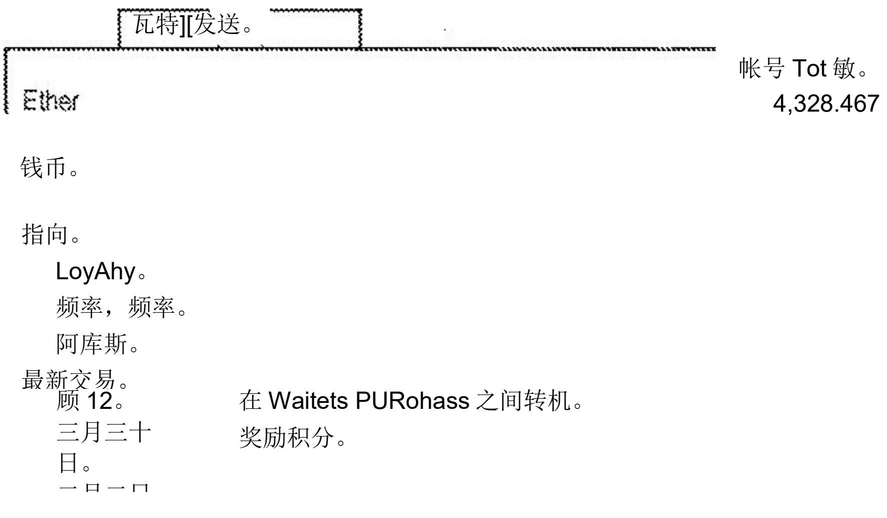
Smart-Smart (Smart^2) Contracts

灯柱^22 件。



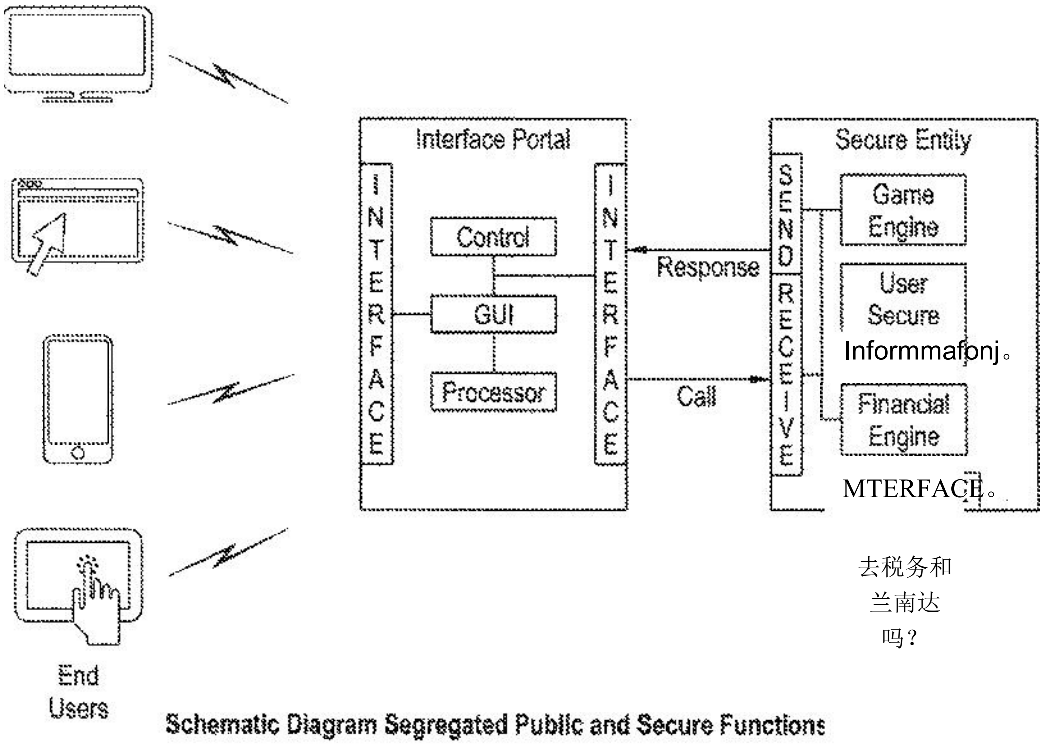
智能内容 WHH 强制参数和可变参数。

RLL^。23



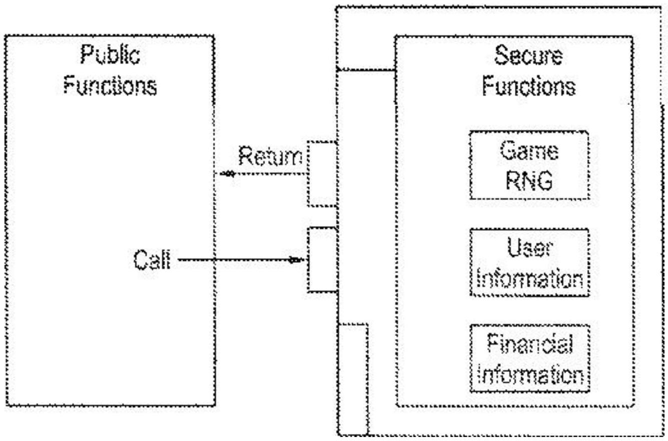
Cryptocurrency Wallet

斜？S *14。*



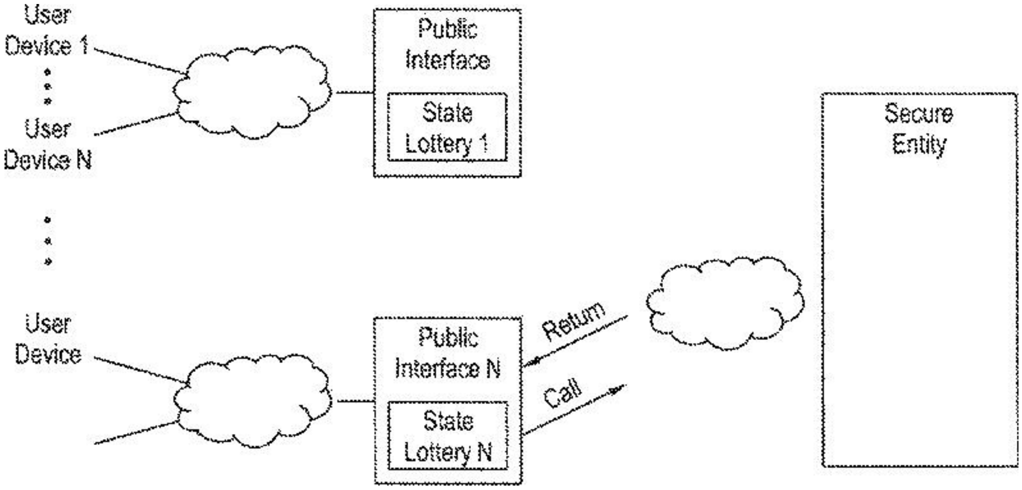
Schematic Diagram Segregated Public and Secure Functions

FIG. 25



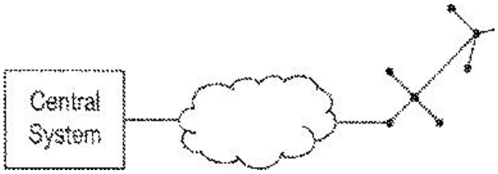
给 Rnandal Instuttans。

分离的安全功能和公共功能的接口。



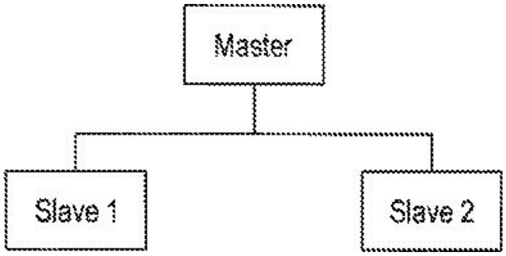
Network Implementation of Segregated Secure and Public Functions

FIG. 27



中心夺系统。

图 28。



系统。

第一张 OSA 彩票。

：|ZP 耳 Joseph A，Smsth。

好了！
：　TrnrrTr TrrTrr^ftrnTTt ffflTrrr。

07/21。

与彩票挂钩的信用卡。

々/i。

用于程序定义状态系统的体系结构、系统和方法。

优先权申请。

[0001]这是申请序列号的延续。其要求于 2017 年 2 月 3 日提交的临时申请 No.62/454,423 的权益，该临时申请通过引用结合于此，如其在此完全阐述的那样，该临时申请于 2017 年 2 月 3 日提交，其权利要求为 62/454,423 号临时申请的利益，该临时申请以引用方式并入本文中。

本发明的领域。

[0002]本发明涉及用于以编程方式控制的娱乐状态系统的体系结构、系统和方法。更具体地，涉及利用认知计算进行程序控制的体系结构、系统和方法，包括但不限于人工智能和机器学习，并且可选地包括分析。提供了系统、方法和体系结构，利用可选地在对等系统中的包括区块链的分散系统来提供 FBR 游戏和娱乐操作。更具体地说，涉及在分散系统中利用诸如比特币的加密货币实现彩票、游戏或娱乐的系统和方法。

发明背景。

[0003]历史表明，为了提供社会和企业的 FBR 高效运作，许多可信系统已经发展。一般来说，这些都涉及对系统的集中控制，以确保遵守规则。在增长空间内，例子包括彩票和受监管的博彩。例如，内华达州博彩管理委员会监督该州博彩管理机构遵守法律法规的情况，并确保该行业公平和高效地运作。

[0004]考虑一下娱乐和游戏系统背景。彩票是一种“国家”职能，充当“信任代理”的罗兰(LoRan)。彩票要素的经典定义是奖金、机会和对价。当这些元素按更正确的时间顺序重新排序时，即首先，收到并持有对价(例如，购票)、机会(例如，确保公平和准确的随机数生成器)和奖品(即，将奖金支付给真正的获胜者)。因此，国家充当一个“信托代理人”，因为它持有对价，保证“4 次机会”的随机性，并支付奖金(所有权转让)。“信任”是建立在系统运营者和监管机构的诚信和可信度的基础上的。彩票或州监管机构往往是前执法人员。人们对此的信任度。监管机构往往基于时间和往绩记录，内华达州的监管系统被认为是高度值得信赖和有效的，部分是基于数十年的往绩记录。此外，在监管过程中失去信任最容易造成企业损失的州最有动力提供监管。这样的系统基于对系统的集中控制。

[0005]赌场是一种四国管制的功能，是一种经过验证的“委托代理”形式。它们由国家颁发许可证，并接受国家检查。

[0006]在游戏和娱乐环境中取得了各种进步。现将以下内容转让给本合同的受让人，特此并入。通过引用好像在此完全阐述：游戏，以及在机会游戏和技能游戏中改进游戏的方法，美国帕特。第 6,565,084 号，游戏，以及 FBR 游戏的方法和设备。玩机会游戏，美国帕特。第 6,488,280 号，游戏，以及 FBR 在机会游戏中的方法和设备，美国 PAT。编号 6,811,484，设备和方法 FBR Game play in a Electronic Environment，U.S.PAT。编号 8,393,946，设备、系统和方法 FBR Implementing Enhanced Gaming and Priking PaRameters in a Electronic Environment(在电子环境中实现增强型游戏和奖励参数的 FBR)，美国专利。编号 7,798,896，设备、系统和方法 FBR Implementing Enhanced Gaming，and Priving PaRameters in a Electronic Environment，U.S.PAT。编号 8,241,110，方法和设备 FBR 增强彩票和游戏环境中的游戏，美国专利。编号 8,727,853，方法和设备 FBR Enhanced InteRactive Game Play in Lotting and Gaming Environment，U.S.PAT。No.8,241,100，Method and System FBR Electronic InteRaction in a Multi-Player Gaming System(多玩家游戏系统中的 FBR 电子交互)，美国专利。8,535,134 号。通常，它们由一套工具组成，以使系统更具吸引力，并优化结果。

[0007]大型系统中的一个令人烦恼的问题是系统不兼容。各种组件通常来自不同的供应商。通常缺乏互操作性和不兼容性。游戏生态系统中的各种系统需要互操作，包括但不限于：游戏运营、营销、CRM(客户关系管理)、忠诚度计划。辅助积分或积分、系统分析和优化以及帐户和审计功能。

[0008]软件定义系统是在更高级别的软件控制下互操作的模块集合。它们通过抽象较低级别的功能来管理网络服务。一般来说，存在应用平面、控制平面和数据平面。示例包括具有控制平面的软件定义网络，该控制平面提供对由相对较不智能的交换机、路由器、存储器组成的数据平面的智能控制。另一个例子是软件定义的无线电。控制平面监视和监督数据平面中频段的使用。

[0009]另一个组件是使用静态接口和工具。例如，API 或应用编程接口通常包括静态接口。它们定义了信息请求的格式 FBR。“如果你以特定的方式询问 FBR X，我们会提供 Y ‘。一般情况下，除通过 API 外，请求者不提供对系统的任何访问。还有一个系统是 SDK，即软件开发工具包(Software Development Kit)。它们可能是静态的。提供了实现预期结果的工具。GDK 或游戏开发工具包也可以是静态的，并提供 FBR 游戏开发工具。

[0010]娱乐或游戏的设计通常由度量驱动的设计驱动。这通常涉及 A/B 测试，比较多个系统之间的结果或优惠度。此外，他们经常监测多变量反应系统。

[0011]彩票和乐透风格游戏的一个方面是它们往往是静态的。在最极端的例子中，它们是字面上印在纸板上的。更一般地，一旦彩票游戏选择了一种格式，例如 49 种格式中的 6 种，就很难改变。公众对变化的看法是，这个游戏对玩家变得不那么有利了。

[0012]赌博问题一直困扰着博彩业。这是 FBR 社会的一个重大问题。而用户可以。

在寻求帮助(例如，1-800-赌博)的情况下，通常会有拒绝和不愿意寻求帮助的情况。已经进行了各种尝试来限制滥用，例如在一些在线游戏中使用速率限制。

[0013]在从实体领域向在线和网络领域转移的过程中，身份问题激增。问题包括：你是你声称的那个人吗？用户的身份会被泄露吗？

[0014]认知智能和适应性智能取得了重大进展。例如，IBM Watson 在 2011 年与高技能选手举行的“危险边缘”(Jeopardy)比赛中获胜。深度学习和模式识别已经出现。目前的趋势包括大数据、模式识别和机器学习。

[0015]在 2D 和 3D 空间中的目标检测方面也取得了最新进展。大规模视觉识别挑战赛(LSVRC)中的一项挑战在 ImageNet 2016 中提供了 FBR 对象检测。ImageNet 的自动标签错误率降至不到 3%，而人工操作的错误率约为 5%。

[0016]在基于机器的游戏性能方面也取得了重大进展。2015 年，Google Deep Mind 使用人工智能强化学习系统学习如何玩 49 款雅达利游戏。2016 年，谷歌的 AlphaGo 系统以 4：1 击败了世界上最伟大的围棋选手之一。2017 年，卡内基梅隆大学(Carnegie Mellon University)的 LiBRatus 项目以统计意义上的方式击败了顶级人类选手。

[0017]在基于云的系统方面取得了进一步的进展。功能已经从本地服务器和存储迁移到远程“云”存储。这些系统提供了 FBR 轻松的可扩展性。基于云的系统可以同时运行多个 4 个实例。他们还可以结合软件即服务，包括人工智能(“Al”)。

[0018]物联网(IoT))利用能够向远程位置发送数据和接收命令数据的设备。各种语音控制设备使用人工智能或机器学习(“ML”)，例如 AmAzon Alexa、Google Dot。**[0019]图 1.。1** 示出了示例性的现有技术集中系统。插图。**2** 示出了示例性的现有技术分布式系统。

[0020]在可信分布式系统中取得了进步，例如在使用基于区块链的系统方面。区块链技术的最初披露归功于中本聪(Satoshi Nakamoto)在 2008 年 10 月发布的一份入门读物。该系统提供 FBR 自动信任或系统信任。区块链范式为 FBR 提供了一个利用分散共识的分散系统。这可以在没有中介的情况下以点对点的方式完成。该系统可以被视为在可编程分布式网络上运行软件的节点网络。它有时被称为具有共享状态事务单例机器、基于事务的状态机、消息传递框架、可信对象消息传递计算框架和可信计算。

[0021]区块链和密码学的结合建立了分散共识。权威和信任由分散的虚拟网络提供。共识逻辑通常与应用程序分开。它可以包括分散架构的第一层。

[0022]区块链使用分布式分类帐。“块”由一组新的已接受事务组成。在一个块中释放一批事务，以供。参与的计算机网络。公共区块上连续的、顺序的交易记录创建了唯一的“链”或区块链。此块将发布到所有其他节点。该出版物定期发布，例如每 10 分钟发布一次。

[0023]EtheriUm 是一个开源的 FBR 智能合约平台。就目前的运营而言，EtheriUm 是一个运行智能合同的分散平台：应用程序完全按照编程运行，没有任何停机、审查、欺诈或第三方干扰的可能性。这些应用程序运行在定制的区块链上，这是一种极其强大的共享全球基础设施，可以移动价值并代表财产的所有权。这允许开发商根据长期的指示(如遗嘱或期货合约)创建市场、存储债务或承诺记录、转移资金，而不存在交易对手风险。EtheriUm 还表示，其目标是创建一种可交易的数字令牌，可以用作货币、资产的表示、虚拟份额、成员资格证明或任何东西。这些代币使用标准的硬币 API，因此合同将自动与任何钱包、也使用此标准的其他合同或交易所兼容。流通中的令牌总量可以设置为简单的固定量，也可以根据任何编程规则集进行浮动。总而言之，EtheriUm 表示，它可以建立一个固定供应的可交易令牌，一个可以发行货币的中央银行，以及一种基于谜题的加密货币。

[0024]当前的系统有许多缺点。他们改变和创新的速度很慢。它们通常涉及不能互操作的专有系统。这往往存在政府和/或体制上的偏见。可能会有一个繁琐的监管环境。最后，交易成本往往很高。

[0025]因此，需要在不一致的、通常是专有的系统之间进行 FBR 互操作性。有必要在更全球化的基础上限制 FBR 赌博，包括地理模拟和全球使用率监测 FBR 问题赌博。有必要对 FBR 问题进行赌博检测和补救。需要 FBR 改进分布式系统。

发明内容。

[0026]一方面，本发明包括娱乐状态系统的系统 FBR 控制。首先，应用平面层适于接收关于娱乐状态系统的操作的指令。优选地，应用平面层耦合到应用平面层接口。第二，控制平面层包括自适应控制单元，例如认知计算单元、人工智能单元或机器学习单元。第三，数据平面层包括输入接口以接收来自一个或多个数据源的数据输入。

[0027]提供了 FBR 训练人工智能系统的系统和方法，包括使用一个或多个人类主体对刺激的反应作为人工智能系统的输入。一个或多个显示器朝向人类受试者以向人类受试者呈现刺激。一个或多个检测器用于监视人类受试者对刺激的反应，所述检测器至少包括运动检测器，所述检测器提供输出。耦合分析系统以接收检测器的输出，该分析系统提供对应于人类受试者的反应是阳性还是阴性的输出。神经网络利用分析系统的输出来提供。

当分析系统的输出为正时，用于神经网络训练的正权重；以及当分析系统的输出为负时，用于神经网络训练的负权重。

附图的简要说明。

[0028]图 3.。1 是现有技术集中式系统的示意图。

[0029]图 3.。2 是现有技术集中系统的示意图。

[0030]图 3.。3 是显示应用平面、控制平面和状态数据平面的程序定义娱乐状态系统(FD-ESS)的系统级框图。

[0031]图 3.。4 是 PD-ESS 的应用状态平面层的系统级框图爆炸。

[0032]图 3.。5 是 PD-ESS 控制平面层的系统级框图爆炸。

[0033]图 3.。6 是 PD-ESS 的状态数据平面层的系统级框图爆炸。

[0034]图 3.。7 是生态系统的图解视图，包括接口和互连。

[0035]图 3.。8 是包括图形处理单元(GPU)的神经网络模型体系结构的系统级框图。

[0036]图 3.。9 是神经网络模型体系结构的系统级框图。

[0037]图 3.。10 是包括差异引擎和数据分析器的多个数据集的系统级图。

[0038]图 3.。11 是响应系统显示和检测系统，用于生成训练人工智能(AI)和机器学习(ML)系统的输入。

[0039]图 3..12 是动态系统应用编程接口(D-API)的系统级图。

[0040]图 4.。13 是动态软件开发工具包(d-SDK)的系统级图。

[0041]图 4.。14 是包括区块链和以太网的分布式系统的系统体系结构层级图，图[0042]。**15** 是许可的区块链系统的系统体系结构层级图，

[0043]图 3.。16 是区块链平台的系统架构层级图。

[0044]图 3.。17 是包含开链服务的区块链平台的系统架构层级图。

[0045]图 3.。18 是具有智能合约的去中心化加密货币系统的系统架构层级图。

[0046]图 4.。19 是具有顺序散列值创建的分散系统的系统体系结构层级图。

[0047]图 3.。20 是加密货币彩票的流程图。

[0048]图 3.。21 是智能合约的流程图。

[0049]图 3.。22 是智能-智能(Smart2)合同的流程图。

[0050]图 3.。23 是具有强制和可变参数的智能合同的流程图。

[0051]图 3.。24 是加密货币钱包的图形用户界面(GUI)。

[0052]图 3.。25 是具有分离的公共和安全功能的系统的系统体系结构级示意图。

[0053]图 3.。26 是分离的公共和安全功能的接口的系统体系结构级别。

[0054]图 3.。27 是具有分离的公共和安全功能的系统的网络实现的系统体系结构级别。

[0055]图 3.。28 是集中式和分散式相结合的系统架构层。

[0056]图 3.。29 是分层系统的系统架构级别。

[0057]图 3.。30 是彩票关联信用卡的平面图。

本发明的详细描述

[0058]计划定义的娱乐国家系统的体系结构、系统和方法。

[0059]下面的描述主要结合图 6。**3**、**4**、**5** 和 **6**，但也可适用于其他数字。AR 体系结构被提供给 FBR 一种程序定义的娱乐状态系统。这优选地用于将控制整体体验的系统与定义状态的底层系统分离。第一平面即应用平面提供接口，主要是 FBR 系统侧用户，例如开发者、事件竞赛的组织者、彩票。第二个平面，控制平面，提供 FBR 智能控制，特别是认知计算，包括人工智能和/或机器学习，包括系统随着时间学习的人工智能。TINS 优选地在模块上方提供智能控制层。第三平面，即状态数据平面，为 FBR 娱乐 4 状^{态}模块提供各种机制，优选地包括“核心环路”、元状态，并提供接口 FBR 终端用户以及输入和输出。

[0060]图3..3提供了框图程序定义的娱乐状态系统(PD-ESS)。插图。4 是 PD-ESS 应用平台层的爆炸式增长，包括应用层 GUI(面向开发者、分支机构和慈善机构)。插图。**5** 提供了一个。爆炸 PI)ESS 控制器平面层。插图。**6** 提供爆炸 PD-ESS 状态数据平面层。还包括娱乐状态网元层的爆炸性增长、用户界面 GUI、价值/所有权转移网元的爆炸性增长以及其他功能块的爆炸性增长。

[0061]首先转到应用平面层，程序用于向 PD-ESS 控制器传达要求和期望行为，它通过 PD-ESS 应用控制器接口(ACI)在 PD-ESS 应用和 PD-ESS 控制器之间提供通信。可选地提供应用程序逻辑和驱动程序。应用层可以接收状态数据平面动作的抽象视图。PD-ESS 应用程序可以与更高级别的抽象控制接口。该系统包括一个接口，即 PD-ESS 应用控制器接口(ACI)。优选地，该管理和管理提供以下内容：(1)到/从应用平面，它提供合同和 SEA，(2)到/从控制平面配置策略，监视性能，以及(3)到/从数据平面元素设置。

[0062]第二转到控制平面层，PD-ESS 控制器在理想的逻辑上是集中式实体，优选地用于将 PD-ESS 应用的要求转换到状态数据平面层，并向应用层提供状态数据平面中的动作(例如，事件信息和统计信息)。控制平面可以从以下位置提供统计数据、事件和状态。

数据平面到应用平面。控制平面优选地在数据平面中的低级控制处实施行为，提供能力发现，并监视统计数据和故障。控制平面有利地包括认知计算，诸如人工智能(Al)和机器学习(ML)，下面将更详细地描述。

[0063]控制平面可以可选地包括分析，包括但不限于模式识别。可以对群体(最好是相关群体)或子集执行分析。优选地，该子集具有与目标用户相似的特征。数据可以根据子集入库。可以分析原始数据的范围。可以包括预测建模。可以在控制平面级别实施负责任的游戏控制，特别是在存在使用率限制和全局限制的情况下。

[0064]第三，转向状态数据平面层，其优选地包括主要子组件和功能网元。可选地，功能网元包括以下部分或全部：1.。娱乐状态网元，2.。价值/所有权转让网元，3.。游戏库，如赌场，VET，电子游戏，锦标赛，有奖游乐设施(AWP)，游戏机制，核心循环，技能，揭秘技能，第二次机会，社交，游戏化，奖品，vGLEP 和奖牌，4.。系统，市场营销，促销，CRM，运营，物流，互动。移动/应用程序和响应式设计，5.。站台，6.。频道，7，彩票，包括零售和中央系统，8。忠诚度，9.。负责任的游戏控制，可选地包括使用速率限制和全局限制(也可以在控制平面层中进行)、10、体育，包括真实世界、梦幻和电子竞技 11 。Other Live Data Entertainment，12。信息和通信技术指的是信息和通信技术，包括网络通信和网络服务，以及 13 管理，包括记录、玩家账户管理、报告、合规，包括合规、安全，包括网络安全、欺诈和风险管理，最好包括审计和支付。

[0065]娱乐状态网元提供与系统用户的接口 FBR 交互。输入从用户选择接收信息。传感器可以是各种形式，包括声音传感器、运动传感器，无论是 2-D 还是 3-D，例如包括微软 Kinect 系统。“内部数据”主要由与游戏操作相关的数据组成。“要与主数据源组合的 ExtemaF 数据源。这些可能包括 1 个。位置，2。当前活动，如驾驶(由车辆提供，由跟踪电话提供)或锻炼(由 FitBit 或类似工具提供)，3.。经济上的。条件，4.。天气,。

5. 最近的事件/新闻，例如，最近的强力球大奖，

6. 营销信息，7.电子邮件扫描，例如，谷歌扫描 Gmail FBR 内容，8.。社交媒体，以及 9.物联网(LOT)。物联网(LOT)提供了各种形式的互联设备，如数据传感器。传感器产生数据输入“刺激”到系统。通过利用任何形式的输入，该系统能够提供 FBR 大规模并行性。对系统的所有数据“刺激”允许系统对所有数据刺激进行自适应和反应。

[0066]输出为用户提供刺激。表单可能包括：1.图像，例如在显示器上，或通过 GUI 或 VR 系统、AR 系统，2.。具有远程计算能力的瘦客户机显示器，3.。投影和全息图，4.声音，5，触觉刺激，6.嗅觉刺激，或 7.直接电刺激，神经或其他。

[0067]价值/所有权转移网元用于接收和转移价值(货币、硬币和其他有价值的物品)，价值可以是指可替代流动资产或其他价值存储。所有权一般指不动产、动产或虚拟财产的所有权。下面详细讨论了区块链、无信任和加密货币系统。

[0068]人工智能(AI)广泛地说是计算机科学中处理智能行为自动化分支。它们是系统，其目标是使用机器来模拟和模拟人类的智能和相应的行为。这可以采取许多形式，包括符号或符号操作 AL。它可以解决分析抽象符号和/或人类可读符号的问题。它可以在数据或其他信息或刺激之间形成抽象连接。它可能会形成合乎逻辑的结论。人工智能是机器、程序或软件所展示的智能。它被定义为智能 Agent 的研究和设计，其中智能 Agent 是一个感知环境并采取行动最大化成功机会的系统。还有一些人将其定义为制造智能机器的科学和工程。

[0069]人工智能通常涉及到神经网络的使用。在各种实施例中，使用神经网络节点的多层堆栈。最低层由颗粒状元素组成。作为游戏应用中的示例，按照更高级别理解的顺序，级别将从单个动作的实例(粒度)、核心循环检测、会话播放、到多会话播放进行。可选地，解析引擎用于将较大的集合(例如数据集或图像)分解或细分为更离散或更细粒度的元素。

[0070]Al 可以具有各种属性。它可能有演绎、推理和问题解决。它可能包括知识表示或学习。系统可以执行自然语言处理(通信)。还有一些人执行感知、运动检测和信息处理。在更高的抽象层次上，它可能会产生社交智力、创造力和一般智力。采用了多种方法，包括控制论和脑模拟、符号、次符号和统计学，以及整合这些方法。

[0071]可以单独或组合使用各种工具。它们包括搜索和优化、逻辑学、概率方法、FBR 不确定性推理、分类器和统计学习方法、神经网络、深度前馈神经网络、深度递归神经网络、深度学习、控制理论和语言。

[0072]Al 有利地在其体系结构中利用并行处理，甚至大规模并行处理。图形处理单元(G U)提供 FBR 并行处理。当前版本的 GPU 可从各种来源获得，例如 NVIDIA、Nervana Systems。

[0073]机器学习被定义为从经验中构建知识的系统，机器学习用于发现模式和规律。

[0074]深度学习使用神经智能。神经网络可以是各种形式的，包括：有效神经网络、矢量化神经网络、矢量化 Logistic 回归、矢量化 Logistic 回归梯度输出、二分类、Logistic 回归、Logistic 回归代价函数、梯度下降、导数、计算图和 Logistic 回归梯度下降。

[0075]深度神经网络(DNN)通常涉及超参数调整。通常，它们利用正则化和最优化。有时它们被称为深度信念网络(DBN)。

[0076]其他形式的神经网络包括卷积神经网络(CNN)或递归神经网络(RNN)，可用系统的示例包括：LS™，亚当，咖啡，辍学，批处理规范，泽维尔/他，蟒蛇，西基特-莱姆和 TensorFlow。

[0077]A1 可以对各种形式的数据集进行操作。数据集可以包括图像，无论是视频图像、2D 数据和/或 3D 数据。可以分析顺序数据。示例包括但不限于自然语言、音频、自动驾驶决策、游戏状态和游戏决策。

[0078]各种工业应用有利地受益于铝的应用。它们包括成像和目标检测，用于识别、分类、挖掘和可选地提供情感分析。其他应用包括自动驾驶。然而，其他应用包括机器人和机器人技术。在医疗保健领域，功能包括成像分析、诊断和游戏化。可以增强各种形式的顺序数据分析，例如语音识别和自然语言处理。音乐应用包括识别和合成。在游戏领域内，应用包括游戏状态序列检测、分析、编队、组合优化和游戏优化。聊天室和机器翻译有利地利用了这些系统。

[0079]图 3.。7 显示了娱乐或游戏生态系统内的组成功能块。附属公司的作用是获得客户。附属公司收取佣金，例如根据获得的用户数量或收入的百分比(%)。可选地，存在到信用卡功能的链接(将在下面结合图进行讨论。**30)。**

[0080]接下来是计划举办彩票、游戏或其他娱乐活动的慈善机构和其他组织。他们提供客户获取服务。他们是活动(游戏、彩票或娱乐)的接受者。他们还收取费用。

[0081]接下来是开发人员，他们提供游戏设计。作为游戏设计的回报，他们获得了多司法管辖区的使用和付费 FBR 的使用。可以提供增强的应用或应用商店，其中可以查看、选择和下载游戏设计。

[0082]接下来，消费者提供注册和标识信息。注册数据可以可选地包括身份、年龄、地址和验证。(可选)数据充足，系统可以通过可选的身份验证级别遵守了解您的客户(KYC)规则。这将存储为永久历史记录。客户获得了玩、赢和接受娱乐的机会。

[0083]接下来是监管机构或信任验证代理。他们提供测试、审批、FBR 游戏公平、整体审批，确保合规和安全。系统授予监管者或信任验证代理对每笔交易(分析仪表板)、玩家帐户、参数、奖金金额和支付以及完整历史记录的访问权限。监管机构或信托验证代理机构获得补偿，无论是费用还是交易金额的一定比例。

[0084]接下来，彩票充当信托代理，并收取交易额的一定比例。可选地，当彩票的历史功能由生态系统内的另一实体执行时，这些功能可以从系统中消除或蒸发。

[0085]无花果。8 和 **9** 涉及 FBR 训练神经网络的学习过程。通过提供重复的输入刺激，然后训练神经网络以提供正确的输出，可以教导系统基于一个或多个输入刺激形成正确的关联输出。在将输入转换为期望输出时，训练可以包括监督学习，例如当目标值和参数被监督时。或者，训练可以是非监督学习，其中系统试图识别输入中具有可识别结构并且可以再现的模式。或者，系统可以使用强化学习，它独立工作(类似于无监督学习)，但根据成功或失败来奖励或惩罚。优选地，强化学习涉及增量改变。在各种训练技术中，可以使用扰动，其中一个或多个输入参数通常以例如小于输入值的 10%、更优选地小于 5%和更优选地小于 3%的扰动量变化，以便监视扰动对输出的影响。在各种训练技术中，可以使用扰动，其中一个或多个输入参数通常以小于输入值的 10%、更优选地小于 5%和更优选地小于 3%的扰动量变化，以便监视扰动对输出的影响。

[0086]超参数和参数可以在 AI 或机器学习系统中使用。模型参数是根据数据自动估计的。可以根据数据估计模型内部的配置变量。这可能是模型在进行预测时所要求的。值定义了模型的技能。它们可以通过数据进行估计或学习。

[0087]超级参数是手动设置的，并在流程中用于帮助估计参数。使用模型外部的配置变量。一般来说，它不能从数据中估计出来。它们经常用于估计模型参数的过程中。它们通常由系统用户指定。通常可以使用试探法设置超参数。它们经常被调整为 FBR，这是一个给定的预测建模问题。超级分类帐可以用作超级分类帐编写器或超级分类帐结构。

[0088]可以在各种类型的硬件上执行人工智能或机器学习。有利的是，支持并行处理的系统可以提供 FBR 计算速度和效率。NVIDIA 和 AMD 提供图形处理单元(GPU)等并行处理单元。麒麟 970、Apple All 和高通 ZEROTH 处理器均配备神经处理单元(NPU)。人工智能和机器学习处理也可以作为云人工智能或机器学习系统提供，如 Google 和 AmAzon Web Services 提供的。**[0089]图 3.。10** 描述了域转换和差异引擎。一个有利的域变换涉及时域到频域(时间序列到频域)。傅立叶级数就是一个例子，它通常用于重复信号，例如振荡系统。傅立叶变换通常用于非重复信号，例如瞬变信号。可以使用诸如快速傅立叶变换(FFT)之类的增强计算技术来提高 FBR 效率和计算速度。然而，另一种域变换是拉普拉斯变换，通常用于电子电路和控制系统。另一种是 Z 变换，通常用于离散时间信号。数字信号处理器(DSP)可以。

被有利地利用。谱密度估计可能包括小波分析、图像分析、数据压缩和多变量分析。有利地使用相关数据集。

[0090]可以使用区分引擎来识别两组或更多组数据之间的区别。该差别可以是基于时间的，例如其中一个数据集与时间 0 有关，而另一组与时间 1、时间 2、时**间** 3、…、**时**间 **N** 有关。可以计算图像中的差别。

[0091]图 3.。11 示出了一个系统，在该系统中，可以监视、捕获和分析受试者的反应，然后将其用作 A1 的输入。在各种努力中，例如在游戏或娱乐设计和创作中，可以监视、分析和使用目标受众的反应来训练人工智能或机器学习系统。受试者对娱乐/游戏刺激的反应用来测量受试者所经历的‘乐趣’，然后该测量(‘FIM’)被用作 A1 或 ML 系统的训练输入。该系统可以检测个体主体行为。或者，该系统可以监视群体行为，用于检测“有趣”的体验，但也可以测量群体或人群的属性，例如兴奋、参与度或基于群体的行为。

[0092]提供显示器作为对一个或多个对象的刺激。可以使用该面板显示器或监视器。可选地，可以利用个人观看设备，例如个人屏幕、虚拟现实耳机、增强现实设备、平视显示器、投影设备或成像技术。

[0093]利用各种检测器来监视一个或多个受试者的反应。运动检测利用运动跟踪硬件和软件。一台照相机拍摄被摄体的图像。各种摄像头包括微软 Kinect、2D 传感器和摄像头以及 3D 传感器和摄像头。度量检测器可以分析身体部位的位置，例如肢体、关节或面部特征。它可以测量速度、运动、位置或运动的更高级别的导数，如变化率。面部探测器监控 FBR 面部识别。可以检测面部属性，例如正面属性(例如微笑)或负面属性(例如皱眉)。可以确定身体位置检测。声音检测可以用麦克风或麦克风阵列来执行。它可以检测声音的属性，例如正面属性(例如，欢呼声)和负面属性(例如，咒骂和嘘声)。利用生物测定扫描检测。生理反应检测可选择性地监测受试者的心率、血压、瞳孔扩张、体温、心电图和精神活动。活动监视检测器监视参与响应，优选地包括投注率、花在显示器上的时间、保留率、重复率和重复参与率。有利地利用了分析。

[0094]系统的输出用作人工智能或机器学习系统的输入。例如，在神经网络中使用强化学习的训练中，正权重使用 FBR 正属性，负权重使用 FBR 负属性。

[0095]该系统还可以提供被识别为与成瘾(例如赌博成瘾)相关联的输出，或者与以其他方式对游戏上瘾的对象相关联的输出。当参与度或轻微上瘾程度被视为可接受时，可以在。当上瘾被认为是不可接受或过度时，可以在训练中使用负权重，而当上瘾被认为是不可接受或过度时，可以在训练中使用负权重。

[0096]人工智能、机器学习、神经网络、在训练 AI/ML 系统中使用用户响应(通常图 2)。**11** 和上面的讨论)可以有利地用于游戏设计和开发、娱乐开发和/或任何创造性开发工作。

[0097]这些系统可以构成工具矩阵。它们可以包括一组给定的工具。从更根本的意义上说，它们包含了一个发现工具的工具。工具可以是游戏状态、娱乐状态或任何形式的状态或物质。

[0098]下面将描述游戏开发，但是工具、系统、方法和架构可以应用于娱乐或任何创造性工作。对于特定的游戏，第一个选项是只提供该特定游戏的基本规则。为了发现获胜的游戏策略，该系统可以与其自身对战，或者与其他系统对战。在另一种选择中，可以向系统提供已知的游戏比特，允许系统使用或忽略游戏比特。在又一备选实施例中，该系统可以配备有游戏库。该系统可以分析游戏库、FBR 游戏元素、游戏机制或核心循环。可选地，系统可以将游戏库的分析限制为类似的游戏，或者可以考虑可选地分成子单元的所有游戏，例如纸牌游戏、棋盘游戏、视频游戏。一旦定义了各种核心循环或游戏元素，系统就可以将它们组合成各种组合和排列，以便定义新的游戏或游戏进行序列。系统可以识别数据中的模式。可以将值分配给各个点或游戏状态或游戏状态决策点的决策。用户响应的使用可以有利地用于游戏形成和优化。用户响应的使用特别适合于强化学习。

[0099]该系统可以以分层方式操作。可以使用分级系统，其中它可以改变一个从属强制参数，只要满足“上级”或“主”强制参数即可。举例来说，可以使用‘超级’强制参数‘来保证特定的结果。可替换地，可以授予管理控制，诸如设置‘top LeveF 约束’。

[0100]系统可以考虑合作动作中的单独功能。职能可能会被重新分配或转移到其他(特别是较低的)行动级别。系统可能会提供新的变量。通过提供分层响应，可以维护核心功能。可选地，该系统可以例如基于来自管理员的命令或基于预定义的标准来使用系统的“终止开关”FBR、凋亡。该系统可以提供诸如处于连续、状态和/或持久状态的体验套餐(Total RecalF)。

[0101]无花果。12 和 13 涉及各种动态的、多变的系统。在名称“d-API”和“d-SDK”中，‘d’代表 FBR 4Dynamic‘，并且能够在系统内和由系统进行更改。交互(请求和/或响应)的格式可以是改变。或者，它可以改变响应中提供的信息的类型、数量或质量。其他可能更改的因素包括请求通过 API 或 SDK 更改信息的能力。可以更改其他操作或管理权限，如只读。

访问、读写、编辑权限、超级管理权限。这些都提供了自适应控制下的 FBR 动态变化。

[0102]在动态应用编程接口(d-API)内，定义了初始格式的 FBR 请求和响应，这可以在 tiSThen 语句中考虑：如果您要求 FBR X 采用商定的格式，则系统将提供 X。动态系统可能会改变格式和/或响应。智能动态更新可以基于人工智能、机器学习或分析。虽然不限于以下，但这些改变中的一些或全部可以动态实现：交互的格式(请求和/或响应)、对更多信息或功能的访问(例如只读)或修改权限、向系统提供信息或数据的能力、以及改变数据的能力。

[0103]在动态游戏开发工具包(d-GDK)中，提供了初始工具包。然后，系统允许动态修改 GDK。优选地，动态修改基于人工智能或机器学习或分析。

[0104]可以提供动态隔离彩票(d-SL)，其中可以提供一个或多个功能单元或彩票。可以使用虚拟化系统，例如在使用虚拟化服务器时。

[0105]无花果。14-20 涉及区块链实现 FBR 游戏、娱乐或其他有用的目的。区块链使用加密的“散列”来识别每个区块和交易。每个连续的块都包含先前代码的散列。这将按时间顺序永久修复事务。区块链同时利用私钥和公钥。先前的散列与随机数一起被添加到新的区块链以形成新的散列，

[0106]加密货币在加密货币是可编程货币或分散价值转移系统上提供 FBR 加密安全交易。它也是一种去中心化的虚拟货币或去中心化的数字货币。

[0107]工作证明或利害关系证明是参与区块链的“权利”。它必须足够繁重，可以在不重做工作的情况下阻止更改。比特币是一种被开采的创造货币，作为 FBR 支付处理工作的奖励，区块链加密货币不涉及交易手续费或购买者支付的费用。没有退款权利或退款。

[0108]它可以在任何形式的网络中实现，既可以是公共的也可以是私有的，可以使用开放软件和专有软件。存储可以是本地存储或云存储和计算。分析可以在本地或在云分析系统中执行。可以执行分析即服务(AAAS)。系统可以是许可的，而不是无许可的分布式系统。

[0109]无花果。21 至 23 **与**智能合约有关。核心要素是，第一，一套承诺，可以是合同的，也可以是非合同的。其次，它们以数字形式指定，以电子方式运行，其中合同条款或功能成果嵌入代码中。第三，它们包括基于协议或技术的基于规则的操作。第四，当事人通过自动履行承诺，以一般不可撤销的方式履行承诺。

[0110]智能合同自动执行不同的过程和操作，在一个实施例中，它们在最终自动执行的基础上自动执行。他们可能会提供。FBR 支付。行动可以以一笔或多笔付款为条件，例如根据付款控制抵押品。

[0111]智能合同可以通过区块链实现。这形成了可在企业对企业实现(B 到 B)和/或对等实现中实现的可信系统。机器对机器的实现允许各种组合。在一个实现中，区块链与构成物联网(LOT)的设备相结合。在另一种组合中，区块链可以与构成物联网的设备与人工智能相结合。通常，该块包含智能合约程序逻辑。它将与特定智能合同相关的消息捆绑在一起，包括输入、输出和逻辑。在又一实施方式中，它们可以提供合约 FBR 差异，例如在使用当前市场价格来调整余额和分散现金流时。

[0112]智能合约是一种信任转移技术。它们降低了交易对手的风险。最好是，这有助于增加信贷。

[0113]智能合同可以在各种模式中实施。它们可能是一份完全用代码写成的合同。它们可以是具有单独自然语言版本的代码中的合同。它们可以是具有编码性能的分裂的自然语言契约。或者，它们可以是具有编码支付机制的自然语言合同。

[0114]智能合同启动需要达成共识。算法构成合同中的每个参与者如何处理消息的一组规则 FBR。它们可以无许可的方式实现，其中任何人都可以提交消息 FBR 处理。提交者可能参与协商一致。或者，他们可以将决策委托给管理员或参与者的子组。另一种实现方式是建立一个允许的系统，其中参与者受到限制。它们通常是预先选定的。然后，他们必须接受门禁进入，并必须满足某些要求和/或管理员的批准。

[0115]智能合同适用于不同的订立方法。他们可以通过协议达成协议，例如在有共同的合作机会或确定的预期结果的情况下。这些可能包括商业惯例、资产互换和权利转让。下一步，条件设置 FBR 合同的启动。这可能是由当事人自己决定的，也可能是由某些外部事件的发生造成的，例如时间、其他可量化的度量或地点。通常，他们会生成一个代码，该代码是用区块链技术加密和链接的。它可以被认证和验证。在执行和处理时，网络更新所有分类帐以指示当前状态。一旦验证和发布，它们就不能更改，只能附加其他块。

[0116]重申一下，智能合同作为具有独立内置信任机制的网络上的分布式应用程序。程序赋予价值单位结合规则 FBR 转让价值单位的所有权。它们充当自动执行程序，自动满足程序化关系的条款。

[0117]图 3.。20 示出了作为智能合约实现的彩票实施例。实现抽奖的方法 FBR 包括以下步骤。设置接收加密货币的时间范围。第二，在时间范围内接收带有所有者标识的加密货币。窗口在指定的持续时间内打开 FBR，然后。

窗口关闭。智能合约例如从随机数生成器生成或接收随机事件。随机数生成器应该包括随机性的算法保证和无黑客攻击的保证。合同在所有者标识相关的加密货币中选择新的所有者(赢家)。然后，它将加密货币的新所有权分配给选定的新所有者(获胜者)。

[0118]智能合同可用于实现核心循环或游戏机制。以下核心循环和游戏机制包括可能实现的部分循环和游戏机制，包括但不限于 Jacko、Poko、Fire Seat、Hi Lo、Rock、Paper、Scissor。在区域和 iLotto 或其他基于阵列或地理的游戏机制或核心循环中。游戏机械师或核心循环的任何子单元本身都可以用作游戏机械师或核心循环。

[0119]Jacko 是一种游戏，包括以下步骤：从具有最小和最大数字的第一数字范围中随机选择目标数字，向玩家呈现目标数字的指示；选择数字 FBr，该数字从具有最小和最大值的第二范围中选择，其中最大值等于或小于第一范围的最小值切；从玩家接收是否再次抽签的指示；如果是，则从第二范围中随机选择一个数字，累加玩家的总抽签次数，重复该步骤，直到玩家拒绝抽签或者总数超过目标数目，并且在玩家拒绝抽签的情况下，从第二范围中随机选择数字，累加这些数字，将它们与玩家的累积量进行比较，并且分配总数目最接近但不超过目标的获胜者。

[0120]Poko 是一个多玩家游戏，其中多个标记被授予预定值，而其他玩家没有关于其他玩家持有的至少一些标记的信息。

[0121]高 LO 是一种包括以下步骤的游戏：对一系列随机抽取的数字执行第一次抽奖选择，从玩家接收下一个随机抽取的数字将高于还是低于前一个数字的指示，如果正确，则奖励与随机抽取的数字的数量相关的奖金，并且继续进行，直到玩家无法预测高/低结果，或者选择停止。

[0122]在该区域中是一种碰运气游戏，该游戏包括以下步骤：在预定义的数字范围内随机选择玩家的目标数字，该范围具有最小和最大；随机选择彩票游戏中使用的一系列数字 FBR，该预定义的数字范围的最小值至少等于该系列数字的最低可能总 FBR 和该预定义范围的最大值的和；通过选择的结论对随机选择的一系列数字进行合计，以及基于玩家人数与总人数的接近程度，将奖金金额分配给玩家人数不超过总数的玩家，

[0123]石头布剪刀是一种具有三个或更多选项的游戏，这些选项相对于彼此具有指定的选项优先级。

[0124]竞争席位是一种增加风险/回报的游戏，包括在 Smart ContRact 中选择退出的能力。多层次机会博弈中 FBR 博弈的一种方法。在最终级别，包括以下步骤：在给定级别呈现多个随机选项，其中至少一个选项是肯定选项，另一个选项是否定选项，以及需要进一步决策的第三选项，接收关于选择多个随机选项中的哪一个的选择，如果选择了肯定选项，则将肯定选项结果与先前肯定选项结果累加，但是如果选择了否定选项，则累加否定选项结果，将累加结果与预定数量进行比较，以及如果累计次数小于预定次数，则重放相同级别，或者如果累计次数等于预定次数，则终止游戏，并且如果选择了第三选项，则接收关于该决定的选择，尊重上述步骤，直到玩家停止，与发生的预定数量的负面事件或最终级别相关。

[0125]iLotto 是基于网格或地理的系统，包括呈现识别对象的网格的显示器 FBR、接收识别对象的玩家选择的输入 FBR、随机选择获胜识别对象的随机生成器 FBR、以及根据规则向玩家奖励积分的计分系统 FBR，所述规则包括：如果玩家选择的识别对象与获胜的识别对象完全匹配，则第一积分值；如果玩家选择的识别对象与获胜的识别对象具有几何关系，则第二积分值；以及如果玩家选择的识别对象与获胜的识别对象具有几何关系，则第二积分值。

[0126]图 3.。23 涉及执行授权参数和可变参数。强制参数在智能合同中设置。强制参数的示例包括支出百分比和支出金额。可变参数受制于强制参数，提供娱乐选项。

[0127]图 3.。24 描述了用于加密的电子存储的钱包。这表示诸如在电话或计算机显示器上的图形用户界面(“GUI”)。各种形式的加密货币可以显示在 GUI 上并存储在钱包中。可以奖励积分，例如 FBR 忠诚度、频率和广播时间。可以列出最近或最近的交易，注明日期、目的和金额。可能会显示总帐户值。

[0128]加密货币系统和智能合约可以与其他系统结合实施。一个额外的系统包括常客或球员的俱乐部系统。它们可能与其他形式的“货币轻量级”相结合，包括微交易和微支付。它们可以与智能资产(即知道其所有者是谁的数字资产或实物)结合使用。数字资产是以数字格式存在的任何东西，通常是二进制格式，并附带使用权。示例包括图像(包括静止图片和视频或动态图像)、可听内容(例如声音、音乐或表演)以及数字文档。所有权通过分布式可信网络控制的财产，例如使用合同的区块链。它们还可以与地理位置结合使用，其中各种组件和建筑组件的物理位置(地理位置)可选地是系统的组件。游戏的地理位置可能会受到限制。该系统可以确保符合数据路由的地理位置。

[0129]无花果。25 至 27 **涉**及具有分离的安全功能和公共功能的系统。这为公共功能和公共实体提供了一个具有多个接口的安全平台。分离的安全功能提供信任代理的功能。安全功能包括以下一项或多项。第一，结果决定。这可能包括使用随机数生成器(RNG)或概率引擎。第二，存储用户或玩家帐户信息。第三，存储货币会计或交易。第四，进行监管和合规接口。第五，开发人员界面等界面。第六，可以提供问答测试、合规性测试和审批等监管职能。

[0130]公共职能包括以下部分或全部。首先，公共系统向安全系统发出‘呼叫’。调用可以通过应用编程接口(API)或 D-API 进行。“open”系统调用调用保护系统 FBR 安全数据。其次，设计器界面用于访问工具、API、开发工具包(DK)和软件开发工具包(SDK)。第三，市场界面充当彩票界面以及可选的应用程序或应用程序商店。第四，操作员接口用于与操作员或组织者(例如慈善机构)对接。它最好服务于出版、营销和销售。第五，用户界面允许注册、播放活动和持久历史记录。

[0131]系统部件可能因功能不同而不同。公共接口和功能优选地包括“开放”平台。这允许 FBR 仲裁并与安全实体就由安全实体执行的游戏操作(例如，可以玩的支付%; vGLEP)和地理位置达成协议。安全实体执行安全功能，包括游戏结果、财务事项和安全用户数据。终端用户利用包括但不限于网络、移动应用、移动网络、平板电脑、计算机、支持显示的设备(无线)、零售商的触摸屏设备(例如，台面游戏)的“频道混合”(Channel Mix)，包括但不限于网络、移动应用、移动网络、平板电脑、计算机、能够显示的设备(无线)、触摸屏设备。私人实体可以施加速率限制并施加负责任的游戏控制。

[0132]无花果。28 和 **29** 描述了混合和分层系统。诸如国营彩票的集中式系统可以与诸如区块链实现的分散式系统相结合。可以在系统内强加分层顺序。在使用强制和可变参数的系统中，可以建立强制参数的分层结构，然后各种可变参数可以服从适当的强制参数。在另一应用中，可以在层次中的较高级别施加全局使用率限制。可以实施分级使用费率限制。系统的各种拓扑结构包括主从式、主从式和循环式。

[0133]图 3.。30 涉及游戏或彩票关联的信用卡和信用卡功能。信用卡和信用功能可以链接到彩票或其他游戏。通过使用信用卡，建立了转换率。例如，FBR 每 100 美元的购买，1 美元的彩票游戏。费率可以是可变的，例如基于机构。在组织或赞助彩票或游戏的慈善组织中，每购买 100 美元，该组织将获得 2 美元的 FBR。拆分也可能。例如，在彩票或游戏中，每购买 100 美元，信用卡所有者将获得 1 美元的奖金，组织将获得 1 美元的奖金。

[0134]在替代实施例中，移动游戏设备可以通过电缆连接到游戏机，或者直接连接到游戏机的端口，或者经由与游戏机通信的网络连接到游戏机。

[0135]用于根据这里描述的实施例对游戏机和服务器进行编程的软件最初可以存储在诸如 CD 或电子存储设备的 ROM 上。这样的 CD 和设备是其上存储有适当的计算机指令的非暂时性计算机可读介质。该程序也可以通过赌场的网络下载到游戏机上。

[0136]应当理解，这里描述的终端、处理器或计算机可以以多种形式中的任何一种实现，例如机架式计算机、台式计算机、膝上型计算机或平板计算机。此外，计算机可以嵌入通常不被认为是计算机但具有适当处理能力的设备中，该设备包括电子游戏机、网络电视、个人数字助理(PDA)、智能电话或任何其他合适的便携式或固定电子设备。

[0137]此外，计算机可以具有一个或多个输入和输出设备。这些设备尤其可以用来呈现用户界面。可用于提供用户界面的输出设备的示例包括打印机或显示屏、输出的 FBR 可视呈现和输出的扬声器或其他声音生成设备 FBR 可听呈现。可用于用户界面的输入设备的示例包括键盘和诸如鼠标、触摸板和数字化平板的定点设备。作为另一示例，计算机可以通过语音识别或以其他可听格式接收输入信息。

[0138]这样的计算机可以通过任何适当形式的一个或多个网络互连，包括作为局域网或广域网，例如企业网或因特网。这样的网络可以基于任何合适的技术，并且可以根据任何合适的协议操作，并且可以包括无线网络、有线网络或光纤网络。如这里所使用的，术语“在线”指的是这样的联网系统，包括使用例如专用线路、电话线、电缆或 ISDN 线路以及无线传输联网的计算机。在线系统包括使用例如局域网(LAN)、广域网(WAN)、因特网以及上述各种组合的远程计算机。合适的用户设备可以连接到网络 FBR 实例、能够通过网络进行通信的任何计算设备，例如台式计算机、膝上型计算机或笔记本计算机、移动站或终端、娱乐设备、与显示设备通信的机顶盒、无线设备(例如电话或智能电话)、游戏控制台等。术语“在线游戏”指的是那些利用这种网络来允许游戏玩家通过远程和本地的联网或在线系统使用和参与游戏活动的系统和方法。例如，“在线游戏”包括通过互联网上的网站提供的游戏活动。

[0139]此外，这里概述的各种方法或过程可以被编码为可在采用各种操作系统或平台中的任何一种的一个或多个处理器上执行的软件。另外，这样的软件可以使用多种合适的编程语言和/或编程或脚本工具中的任何一种来编写，并且还可以被编译为在框架或虚拟机上执行的可执行机器语言代码或中间代码。

[0140]在这方面，实施例可以提供编码有一个或多个程序的有形、非暂时性计算机可读存储介质(或多个计算机可读存储介质)(例如，计算机存储器、一个或多个软盘、光盘(CD)、光盘、数字视频盘(DVD)、磁带、闪存、现场可编程门阵列或其他半导体器件中的电路配置、或其他非暂时性、有形计算机可读存储介质)，当在一个或多个计算机上执行这些程序时。计算机可读介质或介质可以是可运输的，使得存储在其上的一个或多个程序可以加载到一个或多个不同的计算机或其他处理器上，以实现如上所述的各个方面。如这里所使用的，术语“非暂时性计算机可读存储介质”仅包括可被认为是制品或机器的计算机可读介质，并且不包括暂态信号。在此使用的术语“非暂时性计算机可读存储介质”仅包括可被认为是制品或机器的计算机可读介质，并且不包括暂态信号。

[0141]这里一般意义上使用的术语“程序”或“软件”指的是可用于对计算机或其他处理器编程以实现如上所述的各个方面的任何类型的计算机代码或计算机可执行指令集。另外，应当理解，根据本实施例的一个方面，当执行执行方法的一个或多个计算机程序不需要驻留在单个计算机或处理器上，而是可以模块化方式分布在多个不同的计算机或处理器之间，以实现在此描述的实施例的各个方面。

[0142]计算机可执行指令可以是由一个或多个计算机或其他设备执行的多种形式，诸如程序模块。通常，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等。通常，在各种实施例中，可以根据需要组合或分布程序模块的功能。

[0143]此外，数据结构可以以任何合适的形式存储在计算机可读介质中。为简单起见，可以将数据结构示为具有通过数据结构中的位置相关的字段。这样的关系同样可以通过为具有计算机可读介质中的位置的字段分配存储来实现，该计算机可读介质传达字段之间的关系。然而，可以使用任何合适的机制来建立数据结构的字段中的信息之间的关系，包括通过使用指针标签、地址或在数据元素之间建立关系的其他机制。

[0144]这里描述的实施例的各个方面可以单独使用、组合使用，或者在前述实施例和这里描述的概念中没有具体讨论的各种布置中使用。因此，它们的应用不限于前述说明书或附图所示的部件的细节和布置。例如，一个实施例中描述的方面可以以任何方式与其他实施例中描述的方面组合。**[0145]此**外，这里描述的实施例可以提供一种方法，已经提供了该方法的示例。作为该方法的一部分执行的动作可以以任何合适的方式排序。因此，可以构造以与所示不同的顺序执行动作的实施例，这可以包括同时执行一些动作，即使在说明性实施例中被示为顺序动作。

[0146]虽然已经参考其某些示例性特征描述了实施例，但是本领域技术人员可以对所描述的实施例进行各种修改。这里使用的术语和描述仅用于说明，并不意味着限制。具体地说，尽管已经以示例的方式描述了实施例，但是各种设备将实践在此描述的创造性概念。已经以各种术语描述和公开了实施例，实施例的范围不打算也不应该被认为受其限制，特别是当它们落入这里所附权利要求的广度和范围时，可以由这里的教导建议的其他修改或实施例被特别保留。本领域技术人员将认识到，如以下权利要求及其等价物中定义的那样，这些和其他变体是可能的。尽管出于清楚和理解的目的，通过图示和示例的方式较详细地描述了前述发明，但是根据本发明的教导，本领域的普通技术人员可以很容易地看出，在不背离所附权利要求的精神或范围的情况下，可以对其进行某些改变和修改。

[0147]本说明书中引用的所有出版物和专利在此以引用方式并入，就好像每个单独的出版物或专利被具体地和单独地指示通过引用将其整体并入一样。

参考文献。

[0148]IBM ARM，《2017 物联网商业指数，动态转型》，《经济学人》，智库有限公司 2017，第 1-22 页。

[0149]Crosby 等人的《区块链技术：《超越比特币》，《应用创新评论》，第 2 期，Sutardja Center FBR EntretreURship&Technology，BerkeLey Engineering，2016 年 6 月，第 119 页。

[0150]Fisher，《分散式点对点游戏资产平台，使用智能合同与第三方游戏集成》，2014 年 8 月 4 日，12 页，

[0151]Hinton 等，4《深度信念网络的AFast 学习算法》，神经计算，18,1527-1554,2006。

[0152]Jouppi 等人的《张量处理单元的数据中心内性能分析》，将于 2017 年 6 月 26 日在加拿大多伦多举行的 44*计算机体系结构国际研讨会(ISCA)上发表，第 1-17 页。

[0153]LeCun 等人，《深度学习》，《自然》，第 521 卷，2015 年 5 月 28 日，第 436-444 页，

[0154]Marvin，《区块链 A-Z：关于比特币下的改变游戏规则的技术，你需要知道的一切“，2016 年 6 月 3 日，9 页。

[0155]Marvin，《区块链：《正在改变世界的无形技术》，2017 年 2 月 6 日，32 页。

[0156]Mougayar，The Business BlockChain，第 6-9 页，128-133 页，由 John WiLey&Sons 出版，新泽西州霍博肯。

[0157]Nakamoto，《比特币--点对点电子现金系统》，2008 页。1 比 9。

[0158]Ng，44《人工智^{能}现在能做什么，不能做什么》，《哈佛商业评论》，2016 年 11 月 9 日，5 页。

[0159]O‘Dowd 等人的《IBM’s Open》。区块链，使区块链成为真正的 FBR 企业“，IBM 区块链 2016 年 4 月，第 1-20 页。

[0160]罗南，《深度学习预测托托数字》，巴黎学院，2016 年 4 月 1^{日}，第 1-4 页。

[0161]智能合同联盟，“‘智能合同：12 个使用案例：FBR Business and Beyond， A Technology， Legal&Regulatory Information，由智能合同联盟一与德勤合作准备。数字商会的行业倡议“，2016 年 12 月，第 1-53 页。

[0162]图灵，《计算机器与智能》，思想 49：1950 年，第 433-460 页，

[0163]伍德，《以太：安全分散的通用交易分类账“，宅基地草案，2014 年，第 1-32 页。

[0164]Wu 等，《Google 的神经机器翻译系统：《弥合人机翻译之间的鸿沟》，2016 年 10 月 8 日，第 1-23 页，

[0165]Yli-HUUmo 等人，“区块链技术的当前研究在哪里？系统回顾“，2016 年 10 月 3 日，第 1-27 页。

术语表。

[0166]51%攻击：对比特币网络的攻击，允许攻击者创建欺诈性交易，参见 Double Spend。这是可能的，因为控制了比特币网络 50%以上的散列率意味着攻击者可以在计算上胜过所有其他正在挖掘的人。

一个。

[0167]帐户：帐户具有作为以太状态的一部分维护的固有余额和交易计数。它们还具有一些(可能为空)EVM 代码和与其关联的(可能为空)存储状态。虽然是同质的，但区分两种实际类型的帐户是有意义的：具有空关联 EVM 代码的帐户(因此，帐户余额由 Sonic 外部实体控制，如果有的话)和具有非空关联 EVM 代码的帐户(因此帐户代表自治对象)。每个帐户都有一个单独的地址来标识它。

[0168]地址：比特币地址用于接收和发送比特币网络上的交易，它包含字母数字字符串，但也可以表示为可扫描的 OR 代码。比特币地址也是比特币持有者用来对交易进行数字签名的一对密钥中的公钥(参见公钥)。

[0169]地址；使用 FBR 标识账户的代码，例如 160 位代码。

[0170]协议分类帐：协议分类帐是两个或多个当事人用来谈判和达成协议的分布式分类帐。

[0171]空投：一种在人群中分发加密货币的方法，2014 年初首次尝试使用 AURoRaco in(AURoRaco In)。

[0172]算法：在计算或其它解决问题的操作中要遵循的过程或规则，尤指计算机所遵循的过程或规则。

[0173]备用币：作为比特币替代品提供的 FBR 加密货币的统称。莱特币、羽毛币和 PPCoin 都是替代币。

[0174]反洗钱：反洗钱技术被用来阻止人们非法挪用资金，看起来虽然他们已经赚到了，但 AML 机制本质上可以是法律的或技术的，监管机构经常将 AML 技术应用于比特币交易所，

[0175]App：终端用户可见的应用程序，例如托管在以太浏览器中的应用程序。

[0176]应用程序接口(API)：组件(通常是软件组件)用作彼此通信的接口的规范。可以包括规范 FBR 例程、数据结构、对象类和变量。

[0177]套利：通过在同一资产价格不同的市场之间进行交易而产生的无风险利润。

[0178]ASIC：专用集成电路是专门为完成单一任务而设计的硅芯片。就比特币而言，它们旨在处理 SHA-256 散列问题，以挖掘新比特币。

[0179]ASIC Miner：一种包含 ASIC 芯片的设备，用于挖掘 FBR 比特币。它们可以是插入背板的电路板、带有 USB 连接器的设备，也可以是包含所有必要软件的独立设备，这些设备通过无线链路或以太网电缆连接到网络。

[0180]ASIC 挖掘：许多矿工购买单独的计算设备，完全搁置了 FBR 挖掘。作为另一种选择，他们也可以得到专用集成电路；这是一种专门设计的计算机芯片，用于执行一种特定的功能，在这种情况下，只有一功能，即挖掘计算。ASIC 降低了 FBR 开采所需的处理能力和能源，并可以通过这种方式帮助降低整个过程的成本。不管是不是。ASIC 是指专用芯片本身的一个术语，它集成到现有的计算系统中，或作为独立设备运行，术语“ASIC”通常指的是整个系统本身，而不仅仅是芯片。

[0181]非对称密钥算法：这是用于生成公钥和私钥的算法，公钥和私钥是加密货币交易必不可少的唯一代码。在对称密钥算法中，发送方和接收方都拥有相同的密钥；它们可以私密地加密和交换信息，但是由于双方都拥有解码信息，所以它们不能对彼此保密。使用非对称密钥算法，双方都可以访问公钥，但只有拥有私钥的人才能解密加密；这确保了只有他们才能收到资金。

[0182]证明台账：一种分布式分类帐，提供协议、承诺或声明的持久记录，提供这些协议、承诺或声明已作出的证据(证明)。

[0183]自治时代：在没有人工干预的情况下做出决策并对其采取行动的软件。

[0184]自治对象：仅存在于假设的以太状态中的虚构物体。有一个内部地址，因此有一个关联的帐户；该帐户将具有非空的关联 EVM 代码，仅合并为该帐户的存储状态。

B 类。

[0185]Base58；Base58 将二进制数据编码为文本，并用于编码比特币地址。由中本聪(Satoshi Nakamoto)创建，其字母数字字符不包括“0”。“O”，因为它们很难区分。

[0186]基地检查：Base58 的变体，用于检测比特币地址中的键入错误。

[0187]BIP：“比特币改进建议”的首字母缩写，任何想要改善比特币网络的人都可以提交。

[0188]位：比特币面值的名称，等于 100 Satoshis(1 比特币的**百**万分之一)。2014 年，包括比特币(Bitpay)和 Coinbase 在内的几家公司以及各种钱包应用程序都采用了 BIT 来显示比特币金额。

[0189]比特币(大写)：众所周知的加密货币，基于 ProoSof-Work 区块链。

[0190]比特币(小写)：比特币账本使用的具体技术集合，一种特殊的解决方案。请注意，货币本身就是这些技术之一，因为它为矿工提供了开采的动力。

[0191]比特币(货币单位)：一亿，000,000 个智士。一种分散的数字货币单位，可以用来交易商品和服务。比特币也是替代货币生态系统中的一种储备货币。

[0192]比特币 2.0：比比特币白皮书提出的基本支付系统应用更高级或更复杂的比特币或区块链技术的 FBR 应用。比特币 2.0 项目的例子包括对手方、以太、Blockstream、Sarm、Domus 和 Hedgy。

[0193]比特币自动取款机：比特币自动取款机是一种实体机器，允许客户用现金购买比特币。有很多制造商，其中一些可以让用户出售比特币 FBR 现金。它们有时也被称为“BTM”或“比特币 AVMS”。CoinDesk 维护着一张运营比特币 ATM 机的全球地图和一份制造商名单。

[0194]比特币核心：自 2014 年 3 月 19 日发布 0.9 版以来，比特币 Qt 的新名称。不要与 2013 年 8 月发布的 Objective-C 实现 Core 比特币混淆。

[0195]Bitcoind：使用命令行界面的比特币的原始实现。目前是 BitcoinQt 项目的一部分。根据 UNIX 传统，“D”代表 FBR“守护进程”，用于命名后台运行的进程。

[0196]比特币销毁天数：一个估计 FBR 的“货币的速度，与比特币网络。之所以使用比特币，是因为它赋予了很长时间没有使用 FBR 的比特币更大的权重，而且比起每天的总交易量，它更好地代表了比特币正在进行的经济活动水平。

[0197]比特币投资信托基金：这一私人的开放式信托专门投资于比特币，并代表其股东使用最先进的协议来安全地存储比特币。它为 FBR 的人们提供了一种投资比特币的方式，而不必自己购买和安全地存储这种数字货币。

[0198]比特币 J：迈克·赫恩的一个完整比特币节点的 Jaya 实现。除其他功能外，还包括 SPV 实现。

[0199]BitcoinJS：一个在线的 javascript 代码库使用了 FBR 比特币开发，特别是网络钱包、比特币游戏。O 昭(网址：“BitcoinJ s.org)。

[0200]比特币市场潜力指数(BMPI)：比特币市场潜力指数(BMPI)使用一个数据集对 177 个国家的比特币潜在效用进行排名。它试图展示哪些市场最有潜力采用 FBR 比特币。

[0201]比特币网络：维护区块链的分散的点对点网络。这是处理所有比特币交易的工具。

[0202]比特币价格指数(BPI)：CoinDesk 比特币价格指数代表了符合 BPI 指定标准的全球领先交易所的比特币价格平均值。还有一个 API FBR 开发者可以使用。

[0203]比特币协议：在比特币网络上运行的开源密码协议，它设定了网络如何运行的“规则”。

[0204]BitcoinQt：比特币 Qt 是您的计算机使用的开源软件客户端。它包含区块链的副本，一旦安装，它就会把你的电脑变成比特币网络中的一个节点。还充当“桌面钱包”。**[0205]比特币-**红宝石：朱利安·朗沙德尔(Julian Langschaedel)在鲁比的比特币公用事业图书馆。在 Coinbase.com[0206]比特币情绪指数(BSI)上用于生产：比特币情绪指数是一项衡量个人在任何一天感觉这种数字货币的前景是上升还是下降的指标，该指数是由 Qrious 收集的数据提供支持的。**[0207]比特**币白皮书：这份比特币白皮书是由中本聪(Satoshi Nakamoto)撰写的，并于 2008 年发布在加密技术的邮件列表上。本文详细介绍了比特币协议，中本聪紧随其后，于 2009 年发布了比特币代码。

[0208]比特币白皮书：2008 年 11 月，一篇由中本聪(Satoshi Nakamoto)撰写(很可能是化名)的论文发布在新创建的 Bitcoin.org 网站上，标题为“比特币；一个点对点的电子现金系统”(Bitcon；A Peer-to-Peer Electronic Cash System)。这份长达 8 页的文件描述了使用点对点网络生成“不依赖信任的 FBR 电子交易系统”的方法，并阐述了这种加密货币的工作原理。

[0209]位核：Bitpay 用 JavaScript 编写的比特币工具包。比比特人更完整。

[0210]BitPay：一个支付处理器 FBR 比特币，它与商家合作，使他们能够接受比特币作为支付。

[0211]BitStamp：一种越来越受欢迎的 FBR 比特币交易所。

[0212]区块：这是交易数据的集合，是加密货币的基本要素之一。在进行事务时，会收集每个事务的相关信息 FBR，当收集到的数据达到预定大小时，就会将其捆绑成一个块。区块创建后，尽快由投资者进行 FBR 交易验证；这一过程被称为挖掘。

[0213]区块链：自比特币加密货币开始以来已挖掘的块的完整列表。区块链的设计使得每个区块都包含在其之前的区块上的哈希图。这是为了使它更好地防篡改而设计的。更令人困惑的是，

是一家名为区块链的公司，它有一个非常受欢迎的区块链浏览器和比特币钱包。

[0214]区块减半：[见减半]，即矿工开采一个区块所获得的比特币奖励减半。这大约每 4 年发生一次(准确地说是每 210,000 个区块)。

[0215]块头：包含有关块的信息，如前一个块标头的散列、其版本号、当前目标、时间戳和随机数。

[0216]区块高度：区块高度是指区块链中连接在一起的区块数量。例如，高**度** 0 将是第一个块，也称为创世纪块。

[0217]Blockchain.infb：一种运行比特币节点并显示所有交易和块的统计数据和原始数据的 Web 服务。它还为 Android、iOS 和 OS X 提供了轻量级客户端的网络钱包功能。

[0218]整体奖励：对成功散列事务块的矿工的奖励。这可能是硬币和交易费的混合，这取决于相关加密货币使用的策略，以及是否所有硬币都已成功开采。比特币目前每个区块奖励 25 个比特币 FBR。当一定数量的区块被开采时，区块奖励减半。以比特币为例，门槛是每 21 万个区块。

[0219]引导：技术 FBR 通过几条简单的指令将程序上传到志愿者的计算机或移动设备上，从而启动程序的其余部分。

[0220]交易：在交易平台上运行的软件程序，通过预先编程的交易指令执行买入和卖出指令。

[0221]大脑钱包：[见钱包]一种比特币钱包，它使用一长串单词来保护其硬币。这个“口令”是可以记住的，让钱包所有者只需记住口令就可以花掉比特币。

[0222]BRainwallet.org：基于比特币的实用程序，可以手工进行交易，将私钥转换为地址，并使用大脑钱包。

[0223]BTC：短货币缩写 FBR 比特币。**[0224]购买订**单：当投资者接近交易所并想要购买加密货币时，就会建立买入订单。这些订单可以是非常简单的订单(“我想在比特币上花费 x 美元”)，也可以是复杂的订单，包括订单应该完成的时间范围、价格范围等因素。大多数交易所允许 FBR 在网上输入这些信息，但一些投资者更喜欢直接与交易所代表一起检查脱轨情况。买入订单并不一定能保证你的购买；如果你的价格太低，比如 FBR，除非你做出调整，否则优惠可能会到期而没有得到满足。

C。

[0225]资本管制：这些都是地方性措施，如交易税、限制或其他禁令，政府可以用来监管资本市场流入和流出该国的资金。

[0226]卡萨西乌斯硬币：由迈克・考德威尔生产的实物收藏币。每枚硬币都包含一把私钥。在一个篡改明显的全息图下。“Casascius”这个名字是由一个短语“直言不讳”组成的，这是对比特币本身名字的回应。

[0227]总账：中央分类帐是指由中央机构管理的分类帐。

[0228]更改：非正式名称 FBR 交易输出的一部分，在花费该输出后作为“更改”返回给发送方。由于交易输出不能部分花掉，人们只能将 3 个 BTC 输出中的 1 个 BTC 用于创建两个新输出：一个“付款”输出将 1 个 BTC 发送到收款人地址，另一个“收费”输出将剩余 2 个 BTC(减去交易费)发送到付款人地址。BitcoinQt 总是使用密钥池中的新地址，以获得更好的私密性。Blockchain.infb 会发送到钱包中的默认地址。在使用纸质钱包或大脑钱包时，一个常见的错误是将交易更改到不同的地址，然后不小心将其删除。例如，当在临时比特币 QT 钱包中导入私钥时，进行交易，然后删除该临时钱包。

[0229]检查点：块的散列，在此之前，BitcoinQT 客户端在不验证数字签名 FBR 性能的情况下下载块。检查点通常指的是一个非常深的块(至少有几天)，每个人都清楚该块已被绝大多数用户接受，并且重组不会超过该点。它还有助于保护大部分历史记录免受 51%的攻击，因为检查点会影响主链的确定方式，它们是协议的一部分，必须由替代客户端识别(尽管通过检查点进行重组的风险非常低)。

[0230]圆：Circle 是一项兑换和钱包服务，为全球用户提供存储、发送、接收和交换比特币的机会。

[0231]客户：在台式机、膝上型计算机或移动设备上运行的软件程序。它连接到比特币网络并转发交易。它还可能包括一个比特币钱包(见 Node)。

[0232]云：参考互联网和它可以执行 FBR 任何人的功能，如存储、文件发送和使用应用程序。

[0233]云哈希/挖掘：一种挖掘类型，人们可以付费从云中的其他人那里租用计算机能力，以挖掘比特币或其他加密货币。这是通过出售采矿合同来实现的。CloudHash 也是提供这项服务的企业的名称。

[0234]硬币：一个非正式的术语，意思是 1 个比特币，或者是可以花掉的未花掉的交易产出。

[0235]钱币年代：硬币的年龄，定义为货币数量乘以持有期。

[0236]Coinbase：另一个名字 FBR 是比特币生成交易中使用的输入。当比特币被开采时，它不是来自另一个比特币用户，而是作为对矿工的奖励。这笔奖励被记录为一笔交易，但一些随机数据被用作输入，而不是另一个用户的比特币地址。Coinbase 也是比特币钱包服务的名称，该服务还提供支付处理服务 FBR 商家，并充当从交易所购买比特币的中介 FBR。

[0237]Coinbase.com：基于美国的比特币/美元兑换和网络钱包服务。

[0238]冷藏：存储私钥的最安全方式是将它们保存在“冷存储”中，使其离线。这可能是。

以硬件钱包、U 盘或纸质钱包的形式。这些钱包被称为“冷钱包”。

[0239]集体开采：在挖掘数字货币数据块的过程中投入资源和材料往往被证明是太昂贵的 FBR 个人无法参与的。因此，许多有进取心的企业已经想出了一种方法，让那些原本会被排除在外的矿工更容易负担得起采矿费用。这些公司投资于允许 FBR 高端采矿电力的硬件，然后将这种采矿能力的使用权出租给第三方。作为一名个人矿工，这意味着你可以签署一份合同，允许你通过云计算使用预定数量的采矿能力，而不需要购买或维护这样做所需的处理能力的麻烦或费用。成功挖掘数据块所带来的块奖励将归从集体采矿公司购买合同的个人矿工。

[0240]彩色硬币：拟议的 FBR 比特币附加功能，使比特币用户能够赋予他们额外的属性。这些属性可以是用户定义的，使您能够将比特币标记为股票或实物资产的份额。这将使比特币能够作为代币、FBR 和其他财产进行交易。

[0241]压缩大小：事务和块序列化中使用的可变长度整数格式的原始名称。也被称为“智史的编码”。它使用 1、3、5 或 9 字节表示任何 64 位无符号整数。小于 253 的值用 1 个字节表示，字节 253、254 和 255 表示后面的 16 位、32 位或 64 位整数。较小的数字可以用不同的方式表示。在比特币-红宝石中，它在比特币 J 中被称为 Varint。BitconQt 还具有。更紧凑的表示形式称为 Varint，它与 CompactSize 不兼容，用于块存储。

[0242]确认：将比特币交易成功地散列到交易块中，并巩固其有效性的行为。一次确认大约需要 10 分钟，这是对一个事务块进行散列的平均时间长度。然而，一些更敏感或更大的交易可能需要多次确认，这意味着在交易的区块被散列后，必须对更多的区块进行散列，并将其添加到区块链中。每次在交易的区块之后向区块链添加另一个区块，交易就会再次得到确认。

[0243]确认号：确认号是对交易可能被主链拒绝的概率的度量。“Zero Confirmations‘’表示交易未确认(还没有在任何区块中)。一个确认意味着该交易包含在主链中的最新区块中。两次确认意味着该交易包含在紧挨着最近一笔交易的区块中。事务被反转(“双重花费”)的概率随着“上面”添加更多的块而呈指数级递减。

[0244]已确认交易：已包含在区块链中的交易。交易被拒绝的概率是通过多次确认来衡量的。

[0245]共识要点：时间点-或者根据要添加到分类帐中的记录的集合数量或数量定义的点，同行在此开会以商定分类帐的状态。

[0246]协商一致进程：该流程由一组负责 FBR 维护分布式分类帐的同行组成，用于就分类帐的内容达成共识。

[0247]合同：非正式术语用于表示可能与帐户或自治对象相关联的一段 EVM 代码。

[0248]核心开发人员：从事开源代码 FBR 比特币的程序员。他们没有正式受雇于比特币网络，也没有被比特币网络支付，也不控制比特币网络；但是，他们在比特币网络的 GitHUb 资源页面 FBR 上拥有更高的访问权，比特币网络的主要“参考”版本就是在这里开发的。

[0249]造假：为了实施欺诈行为而模仿某物的行为。这方面的一个例子是用假币购物。

[0250]CPU：中央处理器--计算机的“大脑”。在早期，这些工具被用来对比特币交易进行散列，但现在已经不够强大了。它们有时仍被用来对 FBR 替代币的交易进行散列。

[0251]众包：为实现一个目标而汇集的资源，如由普通民众贡献的信息或金钱。这通常是通过人们可以捐赠的网站在网上完成的。

[0252]加密货币：一种仅基于数学的货币形式。与印刷的法定货币不同，加密货币是通过基于密码学解决数学问题而产生的。

[0253]加密技术：使用数学来创建可用于隐藏信息的代码和密码。将用于验证和保护比特币交易的数学问题用作基础 FBR。

[0254]CSRNG：首字母缩写 FBR“加密安全随机数生成器”，用于生成私钥 FBR 比特币钱包。

[0255]旋风：由公司通过水力压裂数字世界 FBR 他们的数据创建的。

D。

[0256]DAO：首字母缩写 FBR“分散的自治组织”，一个理论上的公司，可以存在于云中，并根据预设的算法开展业务，不需要人工管理。也称为“DAC”。

[0257]黑暗使者：Darksend 是黑币的去中心化混合实现，旨在为黑币用户提供更大的交易隐私/匿名性。

[0258]DDoS：分布式拒绝服务攻击使用攻击者控制下的大量计算机来耗尽中心目标的资源。他们经常在互联网上发送少量的网络流量，以占用目标的计算和带宽资源，从而阻止其向合法用户提供服务，比特币交易所有时会受到 DDoS 攻击。

[0259]深层网络：没有被搜索引擎索引的在线内容使得访问变得困难。互联网上的大部分内容都驻留在深网上，可以使用一种名为 TOR 的程序进行访问。

[0260]滞期费：某些货币惩罚用户囤积 FBR，这是通过滞期费实现的，持有未花掉的硬币要收取 FBR 费用。这项费用会随着时间的推移而增加。**[0261]拒绝**服务[DoS]：是对网络的一种攻击形式。比特币节点通过 24 小时禁止其 IP 地址 FBR 来惩罚其他节点的某些行为，以避免 DoS。此外，一些理论上的攻击，如 51%的攻击，可能被用于 FBR 网络范围的 DoS。

[0262]深度：深度指的是区块链中的一个位置。一笔有 6 个确认的交易也可以称为“6 个街区深”。

[0263]桌面钱包：在您的计算机上存储私钥的钱包，它允许您消费和管理比特币。

[0264]确定性钱包：一种基于从称为种子的单个起始点派生多个密钥的系统的钱包。如果钱包丢失，该种子就是恢复钱包所需的全部，并且可以允许在不知道私钥的情况下创建公共地址。

[0265]难度：这个数字决定了猛击一个新块的难度有多大。它与事务块散列的给定数值部分中允许的最大数量有关。数字越小，生成适合它的散列值就越困难。难度因矿工在比特币网络上使用的计算能力而异。如果 la 昭 e 数量的矿工离开一个网络，难度将会降低。

[0266]数字证书：没有加密和解密操作但用户必须申请(并支付年费)个人证书的保护邮件的代码片段，大多数常见的电子邮件服务都不支持它们(谷歌、Outlook、雅虎)。

[0267]数码商品：数字商品是一种稀缺的、可电子转让的、无形的、有市场价值的商品。

[0268]数字标识：数字身份是个人、组织或电子设备在网络空间采用或声称的在线或联网身份。

[0269]分布式自治企业[DAE]: 几乎不需要或根本不需要传统的管理或层级来创造客户价值和所有者财富。

[0270]分布式应用程序[DAPP]：一套智能合约，将数据存储在房屋列表区块链上。

[0271]分布式资本主义：降低参与门槛。

[0272]分布式台账：分布式分类帐是一种分布在多个站点、国家或机构的数据库。记录一个接一个地存储在连续分类帐中。分布式分类帐数据可以“允许”或“未授权”来控制谁可以查看它。

[0273]双倍支出：花两次比特币的行为。当某人使用比特币进行交易，然后使用相同的比特币从另一个人那里进行第二次购买时，就会发生这种情况。然后，它们说服网络的其余部分仅通过在块中散列来确认其中一项交易。由于比特币网络的运营方式，双重支出并不容易做到，但对于那些接受零确认交易的人来说，这仍然是一个风险。

[0274]粉尘：交易产出小于花费它所需的典型费用[原文如此]。这不是协议的严格部分，因为任何大于零的值都是有效的。BitcoinQt 拒绝挖掘或中继“灰尘”事务，以避免无用地增加未用事务输出(UTXO)索引的大小。

[0275]粉尘交易：一笔交易的比特币数量极少，几乎没有经济价值，但在区块链中占据了空间。比特币开发团队已经努力通过提高网络转播的最低交易额来消除灰尘交易。

E。

[0276]ECDSA：椭圆曲线数字签名算法是用于对比特币协议中的交易进行签名的轻量级加密算法。

[0277]椭圆曲线算术：在二维椭圆曲线上的一组点上定义的一组数学运算。比特币协议使用预定义曲线 secp256kl。以下是对这些操作最简单的解释：您可以将点加减，然后再乘以一个整数。除以整数在计算上是不可行的(否则加密签名将不起作用)。私钥是 256 位整数，公钥是预定义的点 G(“生成器”)与该整数的乘积：A-G*a.结合律允许实现有趣的密码方案，如 Diffie-Hellman 密钥交换(ECDH)：具有私钥 A 和 B 的双方可以交换他们的公钥 A 和 B 计算共享密码点 C：C+A*b=B*a，因为(G*a)(G*b)*a。该点 C 可以用作 AES 加密密钥来保护它们的通信信道。

[0278]4 娱乐：状态、显示、用户体验、刺激(光、声、触觉)、标题/价值转移、游戏[0279]托管：在异步交易期间将资金或资产存放在第三方账户中以保护它们的行为。

[0280]ETF：“交易所买卖基金”的缩写。这些是在股票市场交易的投资基金，跟踪标的资产的价格指数。

[0281]以太浏览器：(也称为 EtherUm Reference Client)类似于简化浏览器(A La Chrome)的界面的跨平台 GUI，它能够托管后端完全基于 EtherUm 协议的沙盒应用程序。

[0282]以太运行时环境：(也称为 ERE)提供给在 EVM 中执行的自治对象的环境。包括 EVM，还包括 EVM 所依赖的世界状态的结构 FBR 某些 I/O 指令，包括 CALL&CREATE。

[0283]以太虚拟机：(也称为 EVM)构成执行模型 FBR 帐户的关联 EVM 代码的关键部分的虚拟机。

[0284]EVM 组件：EVM 代码的人类可读形式。

[0285]EVM 代码：EVM 可以本机执行的字节码。用于向帐户正式指定消息的含义和后果。

[0286]交换：交换不同形式的货币和其他资产的中心资源 FBR。比特币交易所通常用于交换加密货币 FBR 和其他通常为法定货币的货币。

[0287]外部执行者：能够连接到以太节点，但在以太世界之外的人或其他实体。它可以通过存放签署的交易，检查区块链和关联状态，与以太互动。具有一个(或多个)内部帐户。

[0288]额外的随机数：放置在 Coinbase 脚本中的一个数字，每当当前 32 次命中的整数溢出时，该数字由挖掘器递增。当随机数溢出时，这不是继续挖掘所必需的方式，还可以改变事务的 Merkle 树或改变 FBR 使用的公钥，以获得块奖励。

F。

[0289]水龙头：第一次发射替代币时使用的一种技术。预先开采一定数量的硬币，并免费赠送 FBR，以鼓励人们对这种硬币感兴趣，并开始自己开采。

[0290]法定货币：一种凭空创造出来的货币，它之所以有价值，是因为人们说它有价值。由于已知它在洗钱和恐怖活动中的应用，它一直受到监管机构的密切关注。不要与比特币混淆。

[0291]填充或封堵：这是一种使用加密货币交易所发出的简单类型的购买订单。投资者决定他们想要多少货币，以什么价格，并确定订单的截止日期 FBR。然后，交易所将根据这些标准尽最大努力完成订单。如果交易所在截止日期前没有找到合适的匹配 FBR 订单，则订单将被取消且未完成。换句话说，根据这些指导原则并在此时间范围内填写此订单。如果你做不到，就杀了它。

[0292]FinCEN：美国财政部下属的金融犯罪执法网络。到目前为止，FIN-CEN 是对交易所比特币交易实施监管的主要组织。

[0293]叉子：区块链的替代持续版本的创建，通常是因为一组挖掘器开始对一组与另一组不同的事务块进行散列。这可能是恶意造成的，可能是一群矿工获得了对网络的过多控制(参见 51%的攻击)，可能是由于系统中的一个漏洞，也可能是由于核心开发团队决定在新版本的客户端中引入大量新功能时故意造成的。根据难度的定义，如果分支成为区块链的最长版本，那么它就是成功的。

[0294]FPGA：现场可编程门阵列(场 ProgRamming Gate ArRay)是一种处理芯片，可以在制造后配置自定义功能。可以把它想象成一块可以写指令的空白硅板。由于 FPGA 可以批量生产并在制造后配置，制造商从规模经济中受益，使其比 ASIC 芯片更便宜。

[0295]FreiCoin：一种基于经济学家西尔维奥·格塞尔(Silvio Gessell)概述的无通胀原则的加密货币。

[0296]无摩擦：就支付系统而言，当交易成本为零或交易限制为零时，系统就是“无功能的”(FHctionless)。

[0297]已满节点：它实现了所有比特币协议，不需要信任任何外部服务来验证交易。它能够下载和验证整个区块链。所有完整节点都实现相同的点对点消息传递协议来交换事务和块，但这不是必需的。完整节点可以使用任何协议并从任何源接收和验证数据。但是，最高的安全性是通过能够尽可能快地与尽可能多的节点通信来实现的。

G。

[0298]燃气：基本网络成本单位。仅由 Ether 支付 FBR 费用(从 PoC-4 开始)，可根据需要自由转换为 Gas。天然气不存在于内部以太计算引擎之外；其价格由交易设定，矿商可以自由忽略天然气价格过低的交易。

[0299]Genesis 区块链中的第一个区块。

[0300]千兆哈希数/秒：给定秒内可能的哈希尝试次数，以数十亿哈希(数千兆哈希)为单位。

[0301]GPU：图形处理单元。硅芯片专门设计了 FBR，这是在现代计算机游戏图形中渲染数百万个多边形所需的复杂数学计算。它们还非常适合加密货币中所需的加密计算。

[0302]图表间隙：有时，市场价值图上的趋势线会出现缺口。这些差距表明，一种商品的价值出现了明显的下跌或上涨，但这并不一定是因为交易而发生的。这可能是闭市、分析师的统计调整或有关大宗商品的强劲消息的结果。有三种类型的间隙：**[0303]1.。**突破缺口，这些出现在强劲的上升或下降趋势的开始，代表着非常大的交易量。

[0304]2.。失控的盖普。这些都发生在上升或下降的趋势中，代表着这一趋势的快速瞬间加剧。

[0305]3.。耗尽差距。这发生在上升趋势或下降趋势接近尾声的时候，并倾向于表明相反方向的小趋势。

H。

[0306]减半：比特币的供应量有限，这使得它们成为一种稀缺的数字商品。比特币的总发行量为 2100 万枚。每个区块产生的比特币数量每四年减少 50%。最后的减半将发生在公元 2140 年。

[0307]硬叉：一些人使用硬叉一词来强调，改变 Bitroin 协议需要绝大多数人同意，否则经济中一些引人注目的部分将继续沿用原有的区块链，遵循旧规则。

[0308]硬件钱包：一种比特币钱包，用于在硬件设备上离线存储用户的比特币。

[0309]哈希：一种采用可变数据量并产生较短的固定长度输出的数学过程。散列函数有两个重要特征。首先，通过查看输出很难计算出原始输入是什么。其次，即使更改输入的最小部分，也会产生完全不同的输出。

[0310]要进行散列，请执行以下操作：来计算某些数据的散列函数。如果没有明确提到散列函数，它是由上下文定义的函数。例如，“对事务进行散列”意味着计算事务的二进制表示的哈希 256。

[0311]使用 RIPEMD-160 进行散列的 SHA-256 用于生成地址，因为它产生的散列(20 字节与 32 字节)比 SHA-256 小，但仍使用 SHA-256 内部 FBR 安全性，即核心比特币中的 BTCHashl60。Hashl60()BitcoinQt。它在脚本中也可以作为 op_HASH160 使用。

[0312]散列，散列 256：当不谈到任意哈希函数时，哈希指的是两轮 SHA-256。也就是说，您应该计算数据的 SHA-256 散列，然后计算该散列的另一个 SHS-256 散列。它用于块头散列、事务散列、创建事务的 Merkle 树或计算地址的校验和。

在核心比特币中称为 BTCHash256O()，在 BitcoinQt 中称为 Hash()。它也可以在脚本中作为 op_HASH256 使用。**[0313]散列**函数：散列函数接受任意输入，例如整数字符串(键)，并输出预先指定长度的值(散列)。比特币使用加密散列函数来保护网络安全。

[0314]哈希率：比特币挖掘者在给定时间段(通常为一秒)内可以执行的哈希数。

[0315]哈希类型(哈希类型)：附加到事务输入中的事务签名的单个字节，描述应如何对事务进行散列以验证该签名。影响输出的类型有三种：All(默认)、Single、None 和一个影响输入的可选修改器 ANYONECANPAY(可以与前三个中的任意一个组合)。ALL 要求对所有输出进行散列(因此，所有输出都是带符号的)。SINGLE 清除除索引与输入相同的输出脚本之外的所有输出脚本。没有清除所有输出，因此允许随意更改它们。ANYONECANPAY 删除除当前输入之外的所有输入(允许任何人独立投稿)。实际的行为比这个概述更微妙，您应该检查实际的源代码以获得更多注释。

[0316]高度：请参见块高度。

[0317]热钱包：一种可以主动连接到互联网的比特币钱包。这些都是使用的，FBR“日常”交易，永远不应该持有大量比特币，因为它们的连通性降低了它们的安全性。

[0318]HTML：首字母缩写 FBR“‘HyperText Markup Language(超文本标记语言)”，即编写网页所使用的语言。

[0319]HTTP：“超文本传输协议”的首字母缩写，这是万维网的底层协议 FBR。**[0320]混合**钱包：这是一个加密货币存储和维护系统，是软件钱包(存储在本地计算机上)和 Web 钱包(存储在第三方服务器上)的组合。你的大部分数字货币账户信息都存储在钱包主机的服务器上--除了 FBR 的一个重要细节。您的私钥(唯一标识您的代码)仅存储在您自己的设备上。当您进行交易时，您的私钥在前往 Exchange 服务器的途中被加密，因此他们永远不会知道您的私钥是什么。访问您的私钥还包括密码，同样只有用户知道。如果用户丢失或忘记该密码，对该帐户的访问可能会被拒绝，并且用户可能会永远失去帐户余额。

我。

[0321]工业区块链：保护手表和其他可穿戴设备的交易功能。

[0322]输入：比特币交易中表示比特币支付来源的部分。通常情况下，这将是一个比特币地址，除非交易是世代交易，这意味着比特币是新开采的(参见 Coinbase)。

[0323]接口系统和方法，两台或多台计算机使用它们都能理解的公共语言在诸如因特网的网络上相互交谈。

[0324]密钥：可以指 ART ECDSA 公钥或私钥，或 AES 对称加密密钥。协议本身不使用 AES(仅用于加密 ECDSA 密钥和其他敏感数据)，因此通常单词 Key 表示 ECDSA 密钥。当谈到钥匙时，人们通常指的是私人钥匙。作为公钥的密钥总是可以从私钥派生而来。请参见私钥和公钥。

[0325]密钥池：一些创建新私钥的钱包应用程序随机保留一个未使用的预生成密钥池(默认情况下，BitcoinQT 保留 100 个密钥)。当需要新的密钥时，FBR 更改地址或新的支付请求，应用程序提供池中最旧的密钥，并用新的密钥替换它。该池的目的是确保最近使用的密钥始终备份在外部存储上。如果没有密钥池，您可以创建一个新密钥，收到其地址的付款，然后在备份此密钥之前关闭硬盘。密钥池保证该密钥在使用前几天已经备份。确定性钱包不使用密钥池，因为它们需要备份单个密钥。

[0326]KiLohash/秒：给定秒内可能的散列尝试次数，以数千个散列为单位。**[0327]基穆**托重力井：一种挖掘困难的重新调整算法，创建于 2013 年的 FBR Megaroin，一种替代币。这口井允许在每个区块进行困难的重新调整，而不是每个 2016 个区块 FBR 比特币。这样做是为了回应人们对多池采矿计划的担忧。

[0328]KYC：了解你的客户/客户规则迫使金融机构审查与他们做生意的人，确保他们是合法的。

我。

[0329]洗衣房：比特币也被称为“混合服务”，它们将来自不同用户的资金组合在一起并重新分配，通过混合它们的“污点”，使得追踪比特币的原始来源变得非常困难。

[0330]分类帐：一种仅附加的记录存储，其中的记录是不可变的，并且可能包含比财务记录更多的一般信息。

[0331]所有事项分类帐：区块链可以解决物联网功能正常运行的六个障碍：弹性、健壮、实时、响应、完全开放、可再生、可编辑、创收和可靠。

[0332]杠杆作用：在外汇交易中，杠杆将账户中的实际资金乘以给定的系数，使你能够进行能够带来丰厚利润的交易。通过给予交易员杠杆，交易交易所实际上是借钱给他们，希望它能赚回比借出的佣金更多的钱。杠杆也被称为要求中的最高要求(ma 昭 in Requisition)。

[0333]轻量级客户端：与全节点相比，轻量级节点不存储整个区块链，因此不能完全验证任何事务。轻量级节点有两种：完全信任外部服务来确定钱包余额和交易有效性的节点(如 Blockchain.infb)和实现简化支付验证(SPV)的应用程序。SPV 客户端不需要信任任何特定服务，但比完整节点更容易受到 51%的攻击。请参阅：简化付款验证。

[0334]Litecoin：一种基于解密工作证明的替代币。

[0335]流动性：轻松买卖资产的能力，交易之间的定价大致相同。相当大的买家和卖家群体是重要的 FBR 流动性。缺乏流动性的市场的结果是价格波动，无法轻松确定资产的价值。

[0336]流动性互换：作为加密货币交易所的一种金融工具，流动性掉期是投资者向他人提供贷款进行交易的合约，以换取 FBR 的固定回报。

[0337]LLL：类 Lisp 的低级语言，一种人类可写的语言，使用 FBR 编写简单的合同和通用低级语言工具包 FBR 反编译为。

[0338]锁定时间(锁定时间)：事务中的 32 位字段，表示事务生效的块高度或 UNIX 时间戳。零表示事务在任何块中都有效。小于 500000000 的数字被解释为块号(限制将在公元 11000 年之后达到)，否则为时间戳。

[0339]彩票：被许多州定义为奖赏、机会和对价。

M。

[0340]MAC 媒体访问控制。

[0341]主链：区块链的一部分，节点认为这是最困难的(参见困难)。所有节点存储包括孤儿在内的所有有效块，并在接收到另一个块时重新计算总难度。如果新到达的一个或多个块没有扩展现有的主链，而是从先前的某个块创建另一个主链，则称为重组。

[0342]主网：主要的比特币网络及其区块链。该术语主要用于与 Testnet 进行比较。

[0343]mBTC：千分之一比特币(0.001 比特币)。

[0344]兆哈希数/秒：给定秒内可能的哈希尝试次数，以百万哈希(数千千哈希)为单位。

[0345]Mempool：术语 FBR 是节点存储的未确认事务的集合，直到它们到期或包含在主链中。当重组发生时，孤立块中的事务要么变为无效(如果已经包含在主链中)，要么移到未确认事务池中。默认情况下，bitcoind 节点在 24 小时后丢弃未经确认的事务。

[0346]合并采矿：这允许矿工同时在多个区块链上工作，从而提高了被挖掘的两种货币的散列率(从而提高了安全性)。例如，Namecoin 已经实现了与比特币的合并挖掘。

[0347]Merkle Tree：Merkle 树是一种抽象数据结构，它将数据项的列表组织在散列树中(就像在 Git、MercURial 或 ZFS 中一样)。在比特币中，Merkle 树仅用于组织块内的事务(块头只包含树的一个散列)，因此满节点可以剪除全部耗尽的事务以节省磁盘空间，SPV 客户端只存储块头并验证事务(如果提供了所有中间散列的列表)。

[0348]消息：通过自治对象的确定性操作或事务的加密安全签名在两个帐户之间传递的数据(作为一组字节)和值(指定为以太)。

[0349]留言电话：将信息从一个账户传递到另一个账户的行为。如果目标帐户与非空的 EVM 代码相关联，则 VM 将以所述对象的状态和所操作的消息启动。如果消息发送者是自治对象，则调用将传递从 VM 操作返回的所有数据。

[0350]小额交易：支付少量 FBR 来购买资产或服务，主要是在线支付。小额交易在传统支付系统下很难进行，因为涉及的佣金很高。以 FBR 为例，用你的信用卡阅读一篇在线文章很难花 2 美分。

[0351]矿工：参与任何加密货币网络执行工作证明的计算机。这通常是为了获得大宗奖励。

[0352]采矿：通过使用计算硬件解决密码问题来生成新比特币的行为。**[0353]挖掘**算法：加密货币用来对比特币网络中的交易进行签名的算法，将区块添加到区块链上。

[0354]采矿合同：一种投资比特币挖掘硬件的方法，允许任何人在约定的时间内出租预先指定数量的散列能力。矿业服务负责硬件维护、托管和电力成本，使其成为更简单的 FBR 投资者。

[0355]矿池：一群矿工决定将他们的计算能力结合起来进行 FBR 挖掘。这使得奖励可以在池中的参与者之间更一致地分配。

[0356]铸币厂：Satoshi 通过将比特币的发行与创建新的区块分类账联系起来分发铸币，将铸币的权力交到了同行网络的所有人手中。

[0357]铸币帽：当加密货币矿工处理交易数据块时，他们会因此产生新的硬币。加密货币是一个年轻的行业，其发行人希望有足够的硬币流通，以满足新投资者的加入。这些新硬币的数学设计是以稳定的速度生产，因此货币的价值也将保持相对稳定(就像在任何其他大宗商品市场一样，会有波动，但不会像商品供应极其有限的情况下那样疯狂)。然而，随着时间的推移，硬币创造的数学也被设计为结束，以避免市场过饱和和货币贬值。

[0358]铸币：在证明赌注硬币时奖励使用者的过程。新硬币被铸造，作为 FBR 在一块内验证交易的奖励。

[0359]混合：为了增加个人历史的私密性而与他人交换硬币的过程。有时它与洗钱联系在一起，但严格地说，它与洗钱是正交的。在传统银行业务中，银行通过向所有第三方隐藏交易来保护客户隐私。在比特币中，任何商家都可以对一个人的整个支付历史进行统计分析，并确定一个人拥有多少比特币，比如 FBR。虽然仍然有可能在每个商家的层面上实施 KYC(了解您的客户)规则，但混合允许在商家之间提供关于个人历史的单独信息。最重要的 FBR 混合使用案例包括：1)拿到一份月薪，然后花在小额交易中(4<Cafe 看到数千美元，当你只付 ^{4}美元时)；2)单次付款，并揭示许多小额私人支出的联系(“汽车经销商看到你对咖啡上瘾”)，在这两种情况下，你的雇主、咖啡馆和汽车经销商都可能遵守 KYC/AML 法律，并报告你的身份和转账金额，但他们都不需要知道。

彼此之间。在拿到工资后混合比特币，然后在支付大笔款项之前混合比特币，就解决了这个隐私问题。

[0360]混合服务：一种将你的比特币与其他人的比特币混合在一起的服务，将你发送给比特币的比特币与分隔符输入和输出一起发回给你。混合服务(也被称为 TUmbler)保护了你的隐私，因为它阻止人们追踪你的特定比特币。它还有可能被用于洗钱。

[0361]移动钱包：这是一种运行“移动客户端”的钱包，人们可以在手机和平板电脑上使用比特币钱包，并在移动中进行支付。

[0362]货币政策：另一个突破是保留软件中编程的价值。

[0363]洗钱：试图通过将这些利润转化为看起来合法的资产来“清理”从犯罪活动中赚取的钱的行为。

[0364]M-of-N 多重签名交易：需要 N 个公钥(M 小于或等于 N)时可以使用 M 个签名进行的事务。只包含一个 OP_CHECKMULSIG 操作码且 N 为 3、2 或 1 的多重签名事务被视为标准事务。

[0365]多重签名：多重签名地址允许多方使用公钥部分播种地址。当有人想要花掉一些比特币时，除了他们自己之外，他们还需要这些人中的一些人签署他们的交易。当人们创建地址时，所需的签名数量在开始时就已达成一致。使用多重签名地址的服务具有更强的防盗能力。

n。

[0366]Namecoin：一种替代币，旨在提供传统域名系统(DNS)的替代方案。用户可以通过域名支付来注册.bit 域，可以通过代理服务器访问。

[0367]网络效应：增值当一种商品或服务的使用变得更加广泛时，它的价值就会增加。**[0368]NFC：**近场通信是“近场通信”的缩写，是一种低功耗、短距离的无线通信方法。这可以用于构建 RFID 系统，也是非接触式智能卡(牡蛎卡)和支付系统(PayPass)的用途。最近在 Apple Pay 应用程序中实现了这一功能。

[0369]节点：使用客户端连接到比特币网络的计算机，该客户端将交易中继给其他人(请参阅客户端)。**[0370]随机数：**在对事务块进行散列时用作输入的随机数据字符串。现时值用于尝试生成符合比特币难度设置的数字参数的摘要。每次散列尝试将使用不同的随机数，这意味着在尝试散列每个事务块时会生成数十亿个随机数。

[0371]非标交易：任何非标准的有效交易。默认情况下，BitcoinQT 节点不会中继或挖掘非标准事务(而是在 testnet 上中继和挖掘)。但是，如果任何人将此类事务放入块中，则所有节点都会接受该事务。在实践中，这意味着不寻常的交易需要更多时间才能纳入区块链。如果某种非标准事务变得有用和流行，它可能会被命名为标准，并被用户(喜欢)采用。请参阅标准事务处理。

[0372]诺瓦科因：尽管这种类型的加密货币还没有接近该行业大型参与者的价值或整体投资者数量。诺瓦科因仍在前五名中占有一席之地；考虑到它是在 2013 年 2 月推出的，这还算不错。Novaco in 使用 SCRYPT 挖掘算法，并结合 prooSoSwork 和 prooSof-Start 方法进行挖掘。

O。

[0373]对象：同义词 FBR 自治对象。

[0374]关闭区块链交易：信任方之间发生在区块链之外的价值交换。之所以会出现这些情况，是因为它们速度更快，并且不会阻止区块链。

[0375]账外币种：梅杰铸造的一种货币，在台账上使用。这方面的一个例子是使用分布式分类账来管理国家货币。

[0376]分类帐上币种：一种铸造在分类账上并在分类账上使用的货币。这方面的一个例子是加密货币。

[0377]操作码：脚本操作的 8 位代码。从 0x01 到 0x4B(十进制 75)的代码被解释为要推送到解释器堆栈上的数据长度(操作码后面是数据字节)。其他代码要么做一些有趣的事情，要么被禁用并导致交易验证失败，或者什么都不做(保留 FBR 将来使用)。

[0378]开放网络企业：随着智能合约变得越来越复杂，并与其他合约进行互操作，这就促成了这一点。

[0379]开源：共享一款计算机软件的源代码，允许任何人分发和修改它的做法。

[0380]孤岛：该块不是有效区块链的一部分，而是被丢弃的叉子的管脚。

[0381]场外交易所：交易员之间直接进行交易，而不是依靠中央交易所进行调解的交易所。

[0382]输出：目的地址是比特币交易的 FBR。单个事务可以有多个输出 FBR。

[0383]硬币拥有者：以太选择了这一点作为它的经济设置。涟漪和明星选择了社交网络。

[0384]计算能力的拥有者：智史选择了这个经济模式。这就要求这些矿工要想参与奖励制度，就必须消耗网络之外的一种资源，即电力。

[0385]纸质钱包：包含一个或多个公开比特币地址及其对应私钥的打印页。通常用于安全地存储比特币，而不是使用软件钱包或网络钱包，因为软件钱包可能会被破坏，网络钱包可能会被黑客入侵或干脆消失。一种有用的冷比特币存储形式。

[0386]参与者：可以访问分类帐的参与者：读取记录或将记录添加到、。

[0387]Pay-to-Script 哈希：一种脚本和地址类型，允许使用任意复杂脚本的紧凑散列将比特币发送到该脚本。这允许付款人支付更少的交易费，而不需要等待很长时间 FBR 非标准交易才能包括在区块链中。则在兑换资金时必须由收款人提供与散列匹配的实际脚本。P2SH 地址采用 Base58 校验编码，就像普通公钥一样，并以数字“3”开头。

[0388]对等点：共同承担责任的行为者，负责维护分类账的身份和完整性。

[0389]P2P：点对点。高度互联网络中至少两方之间发生的分散交互。一种替代“中心辐射式”安排的系统，在这种安排下，交易中的所有参与者都通过单一的中介点进行交易。

[0390]许可分类帐：授权分类帐是一种分类帐，参与者必须具有访问分类帐的权限。授权分类帐可以有一个或多个所有者。当添加新记录时，通过有限的协商过程检查分类帐的完整性。这是由受信任的参与者一政府部门或银行执行的，例如 fbr-这使得维护共享记录比未经许可的分类账使用的协商一致过程简单得多。被许可的区块链提供了高度可验证的数据集，因为协商一致过程创建了一个数字签名，所有各方都可以看到。许可的分类帐通常比未经许可的分类帐快。

[0391]电话到电话转接：这是一种移动应用程序功能，允许将信息从一部智能手机即时传输到另一部智能手机。如果两个移动设备用户想要交换数据，并且两个移动设备用户都在手机上安装并激活了此功能，他们只需将设备放在一定距离内即可进行传输。这些有时也被称为“触摸传输”。

[0392]平台交换：这是一个数字货币交易所，限制了它们在投资者之间进行的交易中发挥的作用。大多数交易所都是为了促进这些交易，并使它们更容易进行。该交易所将分流买卖订单，然后将不会匹配任何符合相关订单标准的投资者。他们的算法经过精心设计，使得交易对双方都是安全和公平的。不过，除此之外，交易所并不扮演任何“中间人”或调停角色。这与交易所形成鲜明对比，交易所将以第三方托管交易资金，或者在推进交易之前与两家投资者讨论交易细节。

[0393]池：一群采矿客户，他们共同开采一个区块，然后在他们之间平分报酬。随着难度的增加，矿池是增加成功开采区块的概率的有效方法。

[0394]PPCoin：也就是点对点硬币或点对点硬币。一种使用赌注证明机制和工作证明相结合的替代币。根据桑尼・金和斯科特・纳达尔撰写的一篇论文。

[0395]开采前：在这枚硬币被公布之前，一位密室-瑞尼公司的创始人挖掘了硬币，并向其他可能想要开采这枚硬币的人公布了细节。预采是一种常用的预采技术，尽管并不是所有预采的硬币都是预采的(见 ScamCoin)。

[0396]Primecoin：由 Sunny King 开发的 Primecoin 使用工作证明系统来计算素数。

[0397]私钥(PrivKey)：由用户保密的字母数字字符串，用于在使用公钥进行散列时对数字通信进行签名。就比特币而言，此字符串是专为使用公钥而设计的私钥。公钥是比特币地址(参见比特币地址)。

[0398]流程节点：在芯片制造过程中产生的以纳米为单位的晶体管尺寸。流程节点越小，效率越高。

[0399]活动证明：把工作证明和赌注证明结合起来。

[0400]爆胎证明：这是一种“烧录”一种工作证明加密货币以获得另一种加密货币的方法。这是一种将一种加密货币从另一种加密货币上“自举”的形式，通过将硬币发送到一个可验证的不可消费地址来实现。

[0401]能力证明：要求矿工将相当数量的硬盘分配给采矿。

[0402]存在证明：一项通过区块链提供的服务，允许任何人匿名和安全地存储存在的证明，FBR 任何他们选择的在线文档。这使人们能够证明文档在某个时间点存在，并证明他们对文档的所有权，而不必担心证据会从他们手中夺走。

[0403]桩的证明：工作证明的另一种选择，即你在一种货币中的现有股份(你持有的该货币的金额)被用来计算你可以开采的该货币的金额。

[0404]存储证明：需要挖掘者在分布式云中分配和共享磁盘空间。

[0405]工作证明：一种将挖掘能力与计算能力捆绑在一起的系统。必须对块进行散列，这本身就是一个简单的计算过程，但是在散列过程中添加了一个额外的变量使其更加困难。当成功地对块进行散列时，散列必须花费一些时间和计算工作量。因此，哈希块被认为是工作的证据。

[0406]消费者：生产产品的客户。

[0407]协议演变：区块链是互联网协议自然演变的结果。《连线》解释了 1974 年最初的 TCP/IP 互联网网络协议和 Tim Berner-Lee 的超文本传输协议(HTTP)是如何以与区块链相同的方式发展的，正在演变为下一代互联网，将多种协议捆绑在一起形成未来框架的基础，并“再次观看互联网的诞生”。

[0408]PSP：支付服务提供商。PSP 为希望接受在线支付的 FBR 商家提供支付处理服务。

[0409]P2SH：参见 Pay-to-Script Has。

[0410]公钥(Pubkey)：一个公知的字母数字字符串，它与另一个私有字符串进行散列以签署数字通信。在比特币的情况下，公钥是比特币地址。

问。

[0411]二维码：包含单色图案的二维图形块代表一系列数据、二维码或“快速响应”码，可由摄像头(包括移动电话中的摄像头)扫描，并经常用于编码比特币地址。

R。

[0412]参考实施：比特币 Qt(或位编码)是使用最多的全节点实现，因此它被认为是其他实现的参考 FBR。如果另一种实现方式与位不兼容。

CoinQT 它可能是分叉的，也就是说，它将不会看到与运行 BitcoinQT 的网络的其余部分相同的主链。

[0413]中继交易：相互连接的比特币节点在尽力的基础上相互中继新的交易，以便将它们发送到挖掘节点。有些事务可能不是由所有节点中继的。例如，非标准交易或没有最低费用的交易。比特币信息协议并不是发送交易的唯一方式。也可以直接寄给矿工，自己挖矿，或者直接寄给收款人，让他们转送或挖矿。

[0414]汇款：汇款通常在国际上作为付款或礼物寄出的一笔钱。

[0415]REO 昭，REOI^ANIZATION：当主链中的一个或多个块变为孤立时节点中的事件。通常，新收到的数据块是对现有主链的扩展。有时(每周 4.6 次)几乎同时产生几个相同高度的块，并且 FBR 在短时间内，一些节点可能会将一个块视为主链的顶端，最终将被更难的块所取代。孤立块中的每个事务要么变为无效(如果已包含在主链块中)，要么变为未经确认并移至内存池。如果出现重大错误或 51%的攻击，重组可能涉及重组多个块。

[0416]复制分类帐：具有一个主(授权)数据副本和多个从(非授权)副本的分类帐。

[0417]奖励：矿工可以在新区块中认领的新生成比特币的数量。该区块的第一笔交易允许矿商要求目前允许的奖励，以及从该区块所有交易的所有交易费中收取交易费。奖励大约每 4 年减半 210000 个街区。截至 2014 年 7 月 27 日，奖励为 25BTC(第一次减半发生在 2012 年 12 月)。出于安全原因，奖励不能在 100 个街区之前花掉，这些街区是在现有图书的基础上建造的。

[0418]波纹：可用于转移任何货币(包括用户创建的临时货币)的支付网络。该网络由当局运营的支付节点和网关组成。使用一系列逻辑单元进行支付，并且网络基于信任关系，

%s。

[0419]智史：目前可用的比特币的最小细分(0.00000001 比特币)。

[0420]中本聪：比特币协议的最初发明者使用的名字，他于 2010 年底退出了该项目。

[0421]假币：一种替代币，其唯一目的是让发起人赚钱。Scamcoins 经常使用抽水和倾倒技术，并一起进行预开采。

[0422]脚本：一种紧凑的图灵不完全编程语言，用于事务输入和输出。脚本由类似 Forth 的堆栈机器解释：每个操作都操作堆栈上的数据。大多数脚本遵循标准模式，并对照前一事务输出中提供的公钥验证事务输入中提供的数字签名。签名和公钥都是使用脚本提供的。脚本可能包含 COM。Plex 条件，但永远不能更改正在转移的金额。金额存储在事务输出的单独字段中。

[0423]scriptPubKey：Bitcoind FBR 中的原始名称是事务输出脚本。通常，输出脚本包含公钥(或其 bash：参见 Address)，这些公钥只允许相应私钥的所有者兑换输出中的比特币。

[0424]scriptSig：事务输入脚本的比特码 FBR 中的原始名称。通常，输入脚本包含签名以证明先前交易发送的比特币的所有权。

[0425]加密：SHA-256 的替代工作证明系统，设计为对 CPU 和 GPU 矿工特别友好，而对 ASIC 矿工几乎没有优势。**[0426]密钥**：加密钱包中使用私钥或加密密钥。比特币协议在任何地方都不使用加密，因此密钥通常意味着使用 FBR 签名交易的私钥。

[0427]顺序：事务输入中的 32 位无符号整数，用于将事务的旧版本替换为新版本。仅在锁定时间不为零时使用。直到序列号为 OxFFFFFFFF，交易才被视为有效。

[0428]种子：确定性钱包中使用的私钥。

[0429]自动执行合同：也称为“智能合同”，这些协议在不需要 FBR 人工干预的情况下促进或执行合同义务。

[0430]国家环保总局：欧洲单一支付区。欧盟内部的一项支付一体化协议，旨在使不同银行和国家之间以欧元进行资金转移变得更容易。

[0431]SHA-256：作为 FBR 比特币工作证明系统基础的加密函数。

[0432]侧链：这些都是理论上独立的区块链，与比特币区块链“双向挂钩”。它们可以有自己的独特功能，并可以将比特币发送到它们和从它们接收比特币。

[0433]签名：通过将私钥和公钥散列在一起来证明比特币交易来自特定地址而生成的数字摘要。

[0434]简化支付验证(SPV)：一种无需存储整个区块链(仅区块标头)和不信任任何外部服务来验证事务的方案。每个事务必须存在于 Merle 树中直到根的所有父哈希和兄弟哈希中。SPV 客户端信任最困难的块头链，并可以验证事务是否确实属于某个块头。由于 SPV 不会验证所有交易，51%的攻击不仅可能导致重复花费(就像满节点一样)，而且还会用无处可见的比特币进行完全无效的支付。然而，这种攻击的成本非常高，而且可能比相关产品更贵。BitcoinJ 库在功能上实现了 SPV。(参见 SPV)。

[0435]智能合同：智能合同是以计算机语言而不是法律语言记录条款的合同。智能合约可以由诸如合适的分布式分类帐系统的计算系统自动执行。

[0436]软叉：有时，软分叉指的是软件行为的重要变化，而不是硬分叉(例如，改变挖掘费政策)。请参见硬叉和叉子。

[0437]源代码：开放源码软件，包括管理比特币规则、FBR、移动和所有权的协议，以及保护和验证比特币交易的密码系统。

[0438]投机者：投机比特币或任何其他形式资产价格的个人。旨在通过以不同的价格买卖来赚取利润。

[0439]消耗产量：事务输出只能使用一次：当另一个有效事务从其自己的输入引用此输出时。当另一个事务试图花费相同的输出时，它将被已经看到第一个事务的节点拒绝。区块链作为一种 ProoSof-Work 方案，允许每个节点就哪一笔交易确实是第一笔交易达成一致。当整个事务的所有输出都用完时，就认为整个事务已用完。

[0440]拆分：区块链的分裂。请参见叉子。

[0441]间谍：简化付款验证。比特币协议的一项功能，使节点无需下载完整的区块链即可验证支付。相反，他们只需要下载块头。

[0442]陈旧：当一个比特币块被成功散列后，任何其他试图散列它的人都可能会停止，因为它现在已经“过时”了。他们只是在重复别人已经做过的工作，FBR 没有报酬。这个词也用在矿池中，用来描述已经完成的抨击工作的份额。

[0443]陈旧区块：一个已经解决的区块，因此不能为矿工提供任何奖励，FBR 在它上面做进一步的工作。

[0444]标准交易：有些事务被认为是标准事务，这意味着它们由大多数节点进行中继和挖掘。更复杂的事务可能有漏洞或导致网络上的 DoS 攻击，因此它们被认为是非标准的，不会被大多数节点中继或挖掘。标准和非标准交易都是有效的，一旦被纳入区块链，将被所有节点识别。标准事务处理包括：1)发送到公钥，2)发送到地址，3)发送到 P2SH 地址，4)发送到 N 为 3 或更小的 M-OSN 多重签名事务。

[0445]存储状态：在帐户的关联 EVM 代码运行期间维护的特定于给定帐户的信息。

T。

[0446]污点：当两个地址都持有特定比特币时，对这两个地址关联程度的分析。污点分析可以用来确定 FBR 比特币从已知 FBR 被盗硬币的地址移动到当前地址需要多少步骤。

[0447]目标：一个 256 位的数字，它将上限 FBR 设置为有效的块头散列。目标越低，找到有效人选的难度就越高。最大(最容易)的目标是。
0X00000000FFF000000000000000000000000000000000000000000000000000000000000000000。难度和目标每隔 2016 个区块调整一次(约。2 周)以保持块之间的间隔接近 10 分钟。

[0448]TCP/IP：首字母缩写代表 FBR“传输控制协议(TRansfer Control ProtocorV)、互联网协议(Intemet Protocol)”，是互联网使用的连接协议。

[0449]太哈希数/秒：给定秒内可能的猛击尝试次数，以万亿次猛击(千兆次)为单位。

[0450]测试网：另一种比特币区块链，纯粹用于 FBR 测试目的，

[0451]测试 3：带有另一个创世模块的最新版本的 Testnet。

[0452]时间戳：证明某一数据在某一时间点存在的证据。对于比特币来说，这是交易何时发生的加密证据。

[0453]无令牌分类帐：无代币分类账是指不需要本币操作的分布式分类账。

[0454]TOR：一种匿名路由协议，供想要在网上隐藏身份的人使用。

[0455]硬币总供应量：对于许多加密货币来说，将会出现的硬币总数是有限制的，比特币的总供应量上限为 2100 万枚。

[0456]交易记录：一条数据，由外部演员签名。它表示消息或新的自治对象。交易记录到区块链的每个区块中。

[0457]交易区块：比特币网络上的交易集合，收集成一个区块，然后可以进行散列并添加到区块链中。

[0458]交易数据库：从纯技术角度来看，区块链是交易数据库。散列、键和节点都构成了一个避开集中式存储的分布式数据库。

[0459]交易费：对通过比特币网络发送的一些交易征收的一小笔费用。交易费奖励给成功散列包含相关交易的块的挖掘器。

[0460]交易录入：事务的一部分，其中包含对前一个事务的输出的引用，以及可以证明该输出所有权的脚本。脚本通常包含签名，因此称为 scriptSig。投入完全消耗了之前的产出。因此，如果用户只需要支付某些先前输出的一部分，则事务应该包括额外的更改输出，将剩余的部分发送回其所有者(在相同或不同的地址上)。Coinbase 事务只包含一个输入，该输入带有对前一个事务的零引用和替代脚本的任意数据。

[0461]交易产出：输出包含要发送的金额和允许进一步支出的脚本。脚本通常包含公钥(或公钥的地址、散列)和签名验证操作码。只有相应私钥的所有者才能创建另一个将该金额进一步发送给其他人的交易。在每个交易中，输出金额的总和必须等于或小于所有输入金额的总和。请参见更改。

[0462]TX：请参阅交易记录。

[0463]TXIN：交易记录输入。

[0464]TXOUT：请参阅交易输出。

[0465]无处不在：区块链无处不在；在字母表中，这已经不是什么新闻了。开放源代码，普遍适用的区块链架构，以及它们分发、匿名、保护和保持完美准确的网络交易记录的能力，使这项技术成为既定技术。

[0466]Ubte：一枚微比特币(0.000001 比特币)。

[0467]未确认交易：不包括在任何块中的事务。也称为“O-confirmatorL”交易。未确认的事务由节点中继，并留在内存池中。未经确认的交易会一直保留在池中，直到节点决定将其丢弃、在区块链中找到它、或将其包含在区块链中、或将其包含在区块链本身中(如果它是挖掘器)。看，确认号。

[0468]唯一节点列表：其他区块链，如 Ripple 和 Stella，依赖于社交网络 FBR 共识，并可能推荐新的参与者(即新的节点)来生成唯一的模式列表。

[0469]未经许可的分类帐：比特币等未经许可的账簿没有单一所有者-实际上，它们不能被拥有。未经许可的分类帐的目的是允许任何人向分类帐提供数据，并允许所有拥有分类帐的人拥有相同的副本。这会产生阻力，这意味着没有参与者可以阻止将交易添加到分类帐中。参与者通过就分类账的状态达成共识来维护分类账的完整性。

[0470]UTXO 集合；未使用的事务输出的集合。通常用于讨论如何优化尚未花费的事务输出的不断增长的索引。索引对于有效验证新创建的事务非常重要。即使新事务的速率保持不变，查找和验证未花费的输出所需的时间也会增加。可能的技术解决方案包括更高效的索引算法和更完善的硬件。例如，BitcoinQT 只保存与用户键匹配的输出的索引，并在验证其他事务时扫描整个区块链。一位网络钱包服务的开发者提到，他们维护着 UTXO 的整个索引，当区块链本身只有 GB 的时候，它的大小在 100 GB 左右。一些人寻求社会方法来解决这个问题。例如，通过拒绝中继或挖掘被认为是粉尘的交易(包含的产出小于开采/中继它们所需的交易费)。

[0471]虚荣地址：具有所需模式(如名称)的比特币地址。

[0472]瓦林特：这个术语可能会引起混淆，因为它意味着不同比特币实现中的不同格式。请参见压缩大小。

[0473]货币流通速度：货币流通速度是衡量收到的钱再次花掉的速度的一个指标。对于比特币，我们用“比特币销毁天数”来衡量其速度，这可以表明人们是在囤积比特币还是在消费比特币。

[0474]核查：区块链在没有验证的情况下不会作为分类账工作。这在很大程度上取决于矿工，他们的区块创建软件在将交易捆绑成区块时，会验证交易的散列。在加密货币和银行场景中，支付验证也是至关重要的。这一验证通过分布式网络中的节点通信进行，在发送比特币交易之前，将其与每个节点的区块链数据进行交叉检查。

[0475]维珍比特币：购买比特币作为奖励，FBR 挖掘一个区块。这些还没有寄到任何地方。

[0476]波动性：对交易的金融资产(包括比特币)随时间的价格变动的测量，

W

[0477]钱包：一种存储比特币的方法，供以后使用。钱包持有与比特币地址相关联的私钥。区块链是与这些地址关联的比特币金额的记录。

[0478]钱包：就像纸币和硬币钱包一样，这里是存放数字货币的地方。加密货币钱包有四种类型：

[0479]1.。软件钱包。这些程序是您加载到台式机或笔记本电脑上的程序。

[0480]2.。移动钱包：这些应用程序以您在智能手机或平板电脑上安装的应用程序的形式出现。它们通常包括 OR 代码扫描和电话到电话转账 FBR On-The-Go 交易。

[0481]3.。网络钱包：这些数据通常通过交换获得，并通过云计算存储在第三方服务器上。它们可以被任何计算设备访问。**[0482]4.。**纸质钱包：你的数字货币可以打印出来，通常是以 OR 码的形式，这些硬拷贝的加密货币“账单”可以像传统货币一样保存在实体钱包中。

[0483]电汇：通过电子方式把钱从一个人转到另一个人。通常用于从比特币交易所发送和检索法定货币。

X。

[0484]XBT：**1 比特**币的非正式货币代码(定义为 100 000 000 Satoshis)。一些人建议使用 FBR 0.01 比特币，以避免与比特币混淆。有传言称，彭博社将 XBT 测试为 FBR 1 比特币，但目前只有 XBTFUND FBR Second-Market 的比特币投资信托基金。参见 BTC。

[0485]XRP：XRP 也被称为 Ripple，是一个建立在区块链基础上的全球支付网络，在国际银行销售。Xrp 本身是昭应用程序可以用来表示平面货币、加密货币、商品或任何其他价值单位的原生货币。Ripple 是使用区块链的开放支付协议最古老的例子之一，但也有一长串公司拥有不同的 API、平台和分布式支付网络。德勤(Deloitte)的银行业展望最近发布了一份报告，估计到 2020 年，基于区块链的支付系统可能会与美国自动清算所(ACH)金融交易网络的规模相当。

Z

[0486]零币：一种旨在使加密货币交易真正匿名的协议。

[0487]零确认交易：一种交易，在比特币的传输得到矿工确认并添加到区块链之前，商家很乐意提供产品或服务。它可能会带来重复支出的风险。

[0488]零确认交易：在某些情况下，数据 FBR 加密货币交易的处理可能需要半分钟以上到十分钟以上的任何时间。虽然这对于验证交易是必要的，并防止重复支出等欺诈性活动，但等待时间可能会给参与交易的人带来不便。因此，一些与数字货币打交道的交易所和企业正在提供“零确认”交易，这些交易几乎可以立即得到验证，而无需等待 FBR 挖掘过程。

确认数据块。重复消费，即硬币持有者将同一货币用于两笔不同的交易的做法，是零确认交易的一个令人担忧的问题。由于加密货币没有以任何方式“依附”于消费它的人，当他们的双重支出通过挖掘过程被发现时，他们早就不见了，无法追踪。随着 FBR 零确认交易需求的上升，加密货币行业的企业家们正在寻找立即验证或拒绝交易的方法，而不必等待 FBR 挖掘发生。与此同时，许多企业收取费用，以抵消零确认交易的财务风险，但还有一些企业拒绝接受这些费用，直到技术跟上。)。

[0489]Z 系统：IBM 公开承诺在许多方面推进区块链技术，但该公司甚至为 FBR 开发人员提供了区块链即服务(Baas)平台。IBM Cloud，以及在 IBM a Systems 上集成基于区块链的应用程序(通过 Hyperledger 项目创建)。IBM 甚至计划在 Watson Lot 平台上利用区块链与 Watson 相结合，使来自基于 RFID 的位置、条形码扫描事件或设备报告的数据等设备的 FBR 信息能够与 IBM 的区块链一起使用，并与分布式分类账和智能合约同步。

我们声称：

1. 一种娱乐状态系统的系统 FBR 控制，包括：

应用平面层，所述应用平面层适于接收关于所述娱乐状态系统的操作的指令，所述应用平面层耦合到应用平面层接口，

控制平面层，所述控制平面层包括自适应控制单元，所述控制平面层与所述应用平面层接口对接以接收与关于所述娱乐状态系统的操作的指令有关的信息，所述控制平面耦合到控制平面层接口，以及。

数据平面层，所述数据平面层包括用于接收来自一个或多个数据源的数据输入的输入接口，所述数据平面层耦合到所述控制平面层接口。

2. 该系统 FBR 如权利要求 1 所述的娱乐状态系统的控制，其中自适应控制单元包括认知计算单元。

3. 如权利要求 1 所述的娱乐状态系统的系统 FBR 控制，其中所述控制平面层包括人工智能单元。

4. 如权利要求 1 所述的娱乐状态系统的系统 FBR 控制，其中所述控制平面层包括机器学习单元。

5. 如权利要求 5 所述的娱乐状态系统的系统 FBR 控制，其中控制平面层包括神经网络。

6. 如权利要求 5 所述的娱乐状态系统的系统 FBR 控制，其中所述神经网络是深度神经网络。

7. 如权利要求 5 所述的娱乐状态系统的系统 FBR 控制，其中所述神经网络包括图形处理单元(GPU)。

8. 如权利要求 5 所述的娱乐状态系统的系统 FBR 控制，其中所述神经网络是利用用户响应数据来训练的。

9. 如权利要求 5 所述的娱乐状态系统的系统 FBR 控制，其中所述神经网络是矢量化神经网络。

10. 如权利要求 5 所述的娱乐状态系统的系统 FBR 控制，其中所述神经网络是递归神经网络。

11. 如权利要求 1 所述的娱乐状态系统的系统 FBR 控制，其中所述控制计划层还包括分析单元。

12. 根据权利要求 1 所述的娱乐状态系统的系统 FBR 控制，其中所述控制平面层还包括处理器。

13. 如权利要求 1 所述的娱乐状态系统的系统 FBR 控制，其中所述应用平面层包括图形用户界面单元。

14. 如权利要求 1 所述的娱乐状态系统的系统 FBR 控制，其中所述应用播放层还包括处理器。

15. 根据权利要求 1 所述的娱乐状态系统的系统 FBR 控制，其中所述数据平面层包括输入端口。

16. 如权利要求 1 所述的娱乐状态系统的系统 FBR 控制，其中所述输入端口耦合以接收外部数据。

17. 如权利要求 16 所述的娱乐状态系统的系统 FBR 控制，其中物联网(LOT)数据中的外部数据。

18. 如权利要求 16 所述的娱乐状态系统的系统 FBR 控制，其中所述输入端口耦合到处理器。

19. 如权利要求 1 所述的娱乐状态系统的系统 FBR 控制，其中所述数据平面层包括图形用户界面(GUI)生成器。

20. 如权利要求 19 所述的娱乐状态系统的系统 FBR 控制，其中图形用户界面耦合到输出端口。

21. 根据权利要求 20 所述的娱乐状态系统的系统 FBR 控制，其中所述数据平面层包括适于耦合到显示设备的输出端口。

22. 根据权利要求 1 所述的娱乐状态系统的系统 FBR 控制，其中所述数据平面层还包括值转移元件。

23. 如权利要求 1 所述的娱乐状态系统的系统 FBR 控制，其中所述数据平面层还包括标题传送元件。

24. 根据权利要求 1 所述的娱乐状态系统的系统 FBR 控制，其中所述数据平面层还包括管理网元。

25. 根据权利要求 1 所述的娱乐状态系统的系统 FBR 控制，其中所述数据平面层还包括控制网元。

网络。

(19)美国。

(12)专利**申请公开(10)。编号：美国 2018 年/0373983 Al。**

Katz et al.　　　　(43)酒吧　**日期**　　**2018 年 12 月**

(54)用于程序定义的交易系统和分散的加密货币系统的体系结构、系统和方法。

(71)　申请人：**里程碑式的娱乐。**
有限责任公司，加利福尼亚州贝弗利山庄
(美国)。

(72)　发明者：**兰德尔·M·卡茨(Randall M.Katz)，加利福**
尼亚州贝弗利山。
(美国)；罗伯**特·特切克(Robert Tercek)，**
加利福尼亚州好莱坞(美国)。

(21)　APPL。编号：**16/052,409。**

(22)　提交：　　**2018 年 8 月 1 日。**

相关的美国申请数据。

(63)延续 2018 年 2 月 1 日提交的第 15/886,432 号申请。

(注 60)临时申请第 62/454,423 号，于 2017 年 2 月 3 日提交。

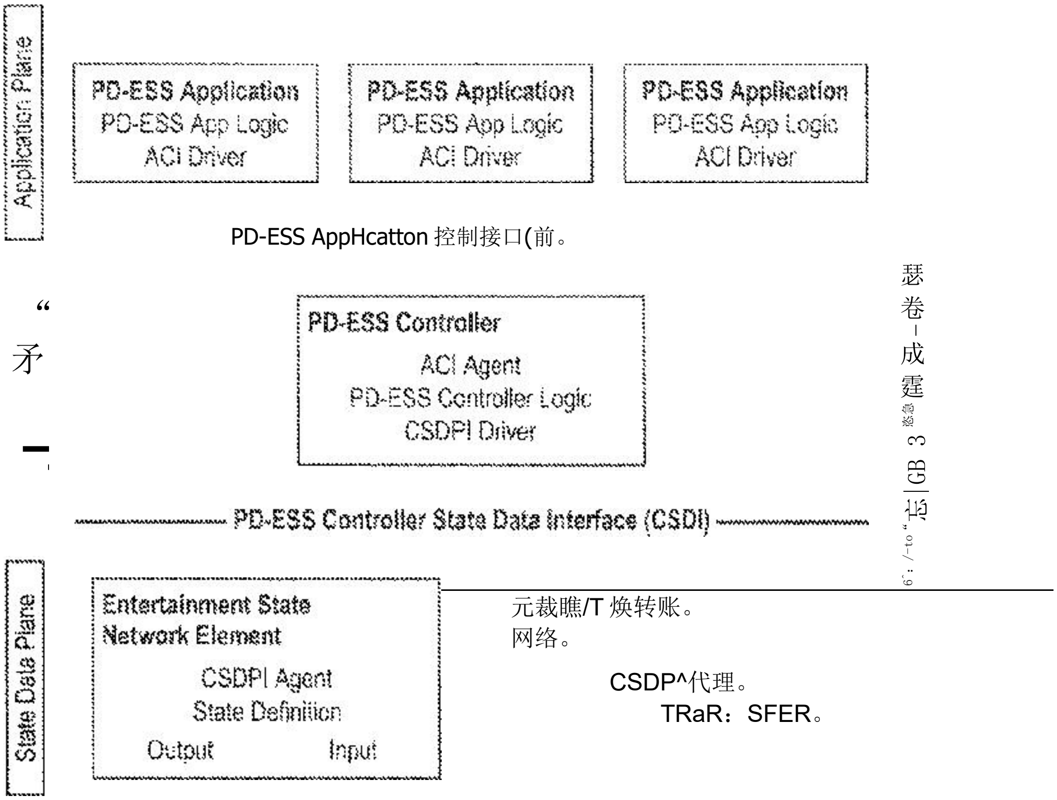
出版物分类。

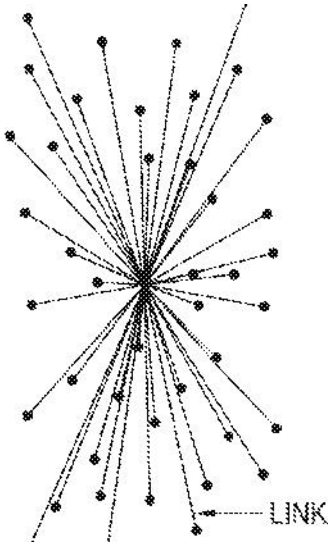
(51)内部。**克莱。**
G06N 3/08(2006.01)。
G07F17/32(2006.01)。
G06Q 20/06(2006.01)。
G06K 9/00(2006.01)。

(52)美**国。**
CPCG06N 3/08(2013.01)；G07F ***17/329。***
(2013.01)；G06K 9/00221(2013.01)；
G06Q20/065(2013.01)。

(57)摘**要。**

一方面，本发明包括一种利用分布式分类账控制交易状态系统的系统。首先，该系统包括适于接收关于事务状态系统的操作的指令的应用平面层。优选地，应用平面层耦合到应用平面层接口。第二，提供控制平面层，该控制平面层包括自适应控制单元，诸如认知计算单元、人工智能单元或机器学习单元。第三，数据平面层包括输入接口，以接收来自一个或多个数据源的数据输入，并提供耦合到分散分布式分类帐的输出，数据平面层耦合到控制平面层。可选地，分散的分布式分类帐存储关于加密货币的数据。





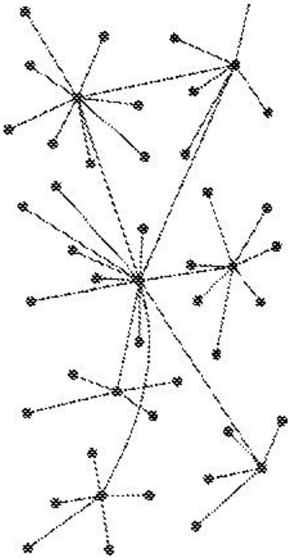
诺伊“。

中央报刊(A)。

现有技术系统。

RF<^«1。

(现有技术)。



分散的。

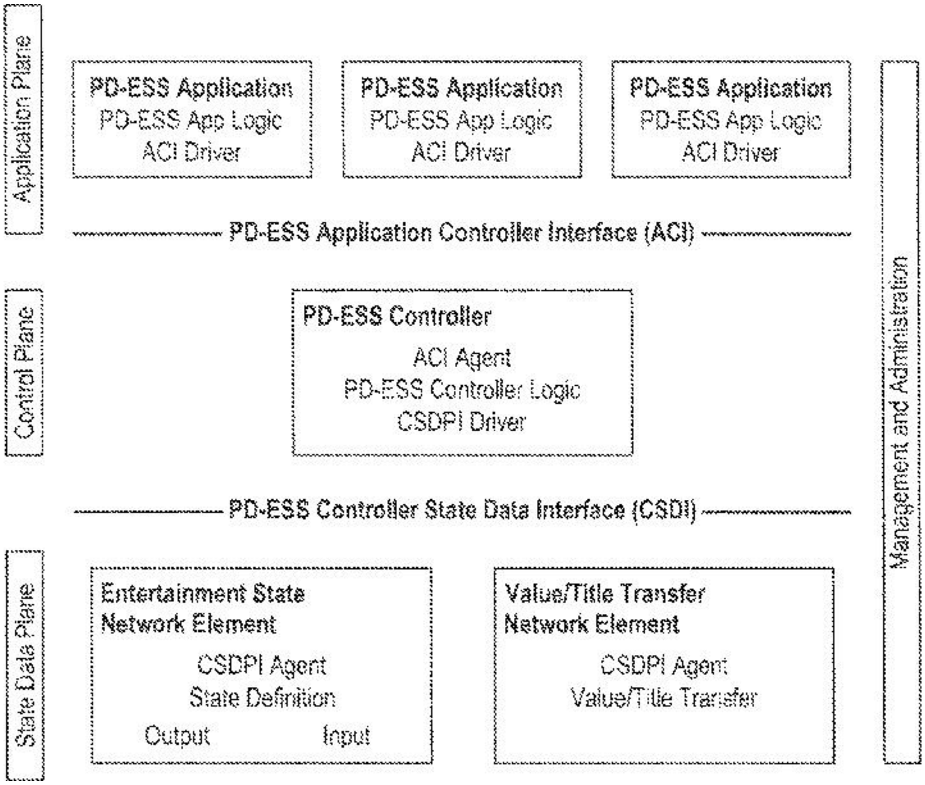
RT S。

整娑严%。

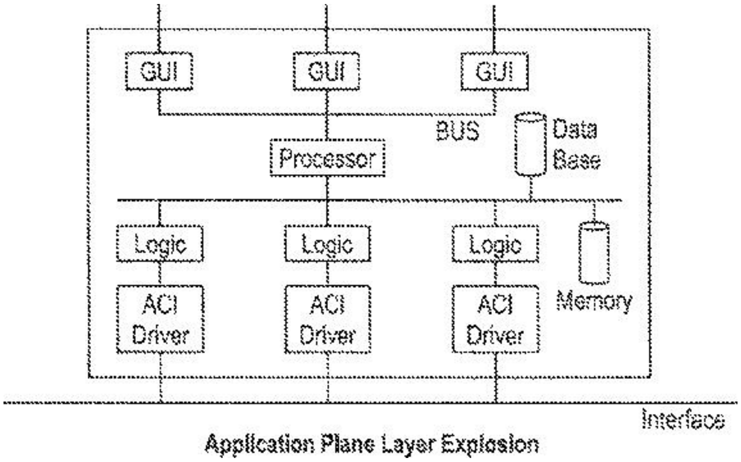
网 S GB。

(现有技术)

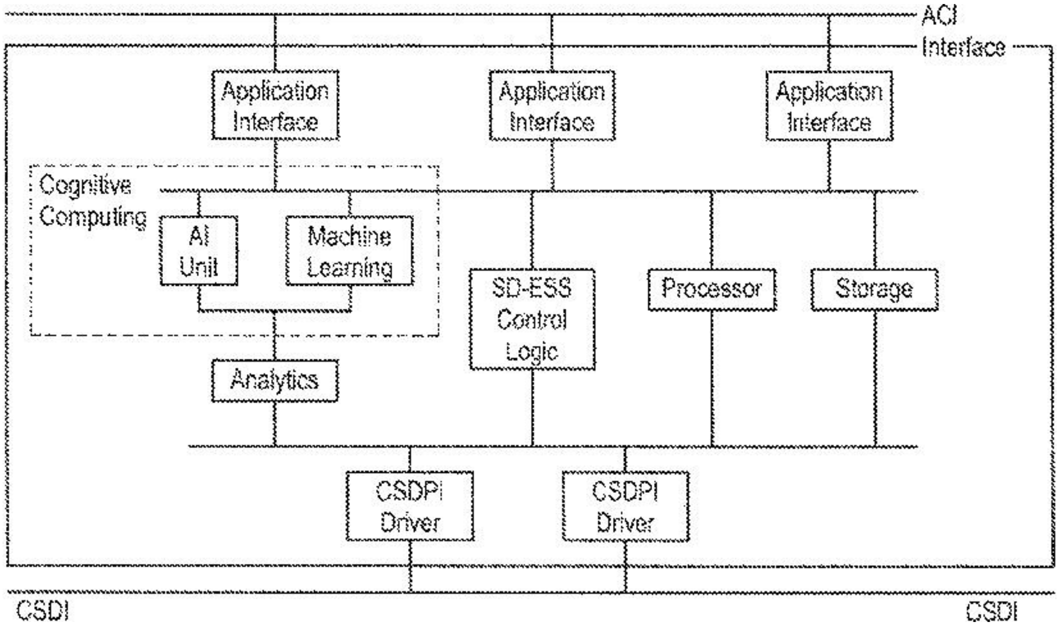
专利申请公布 **2018 年 12 月 27 日美国 2018 年/0373983 年度第 2 页。**

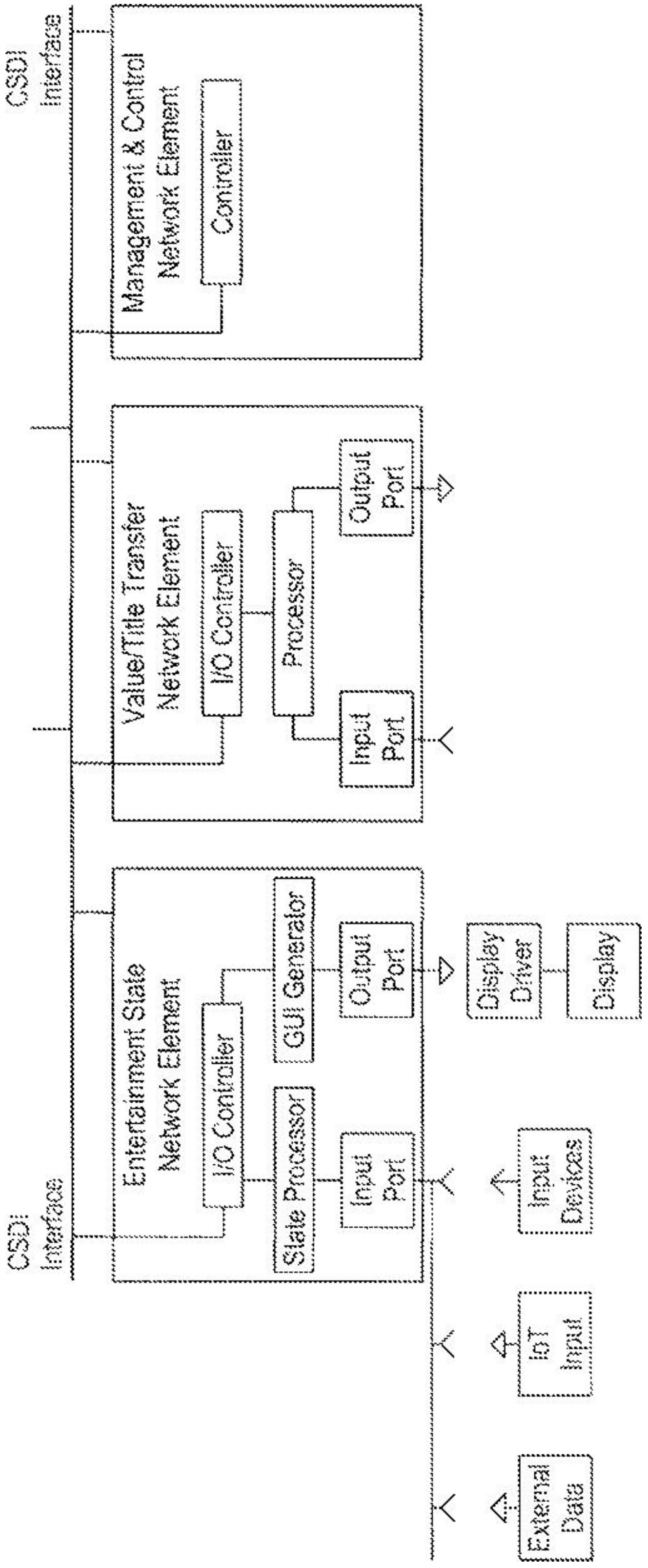


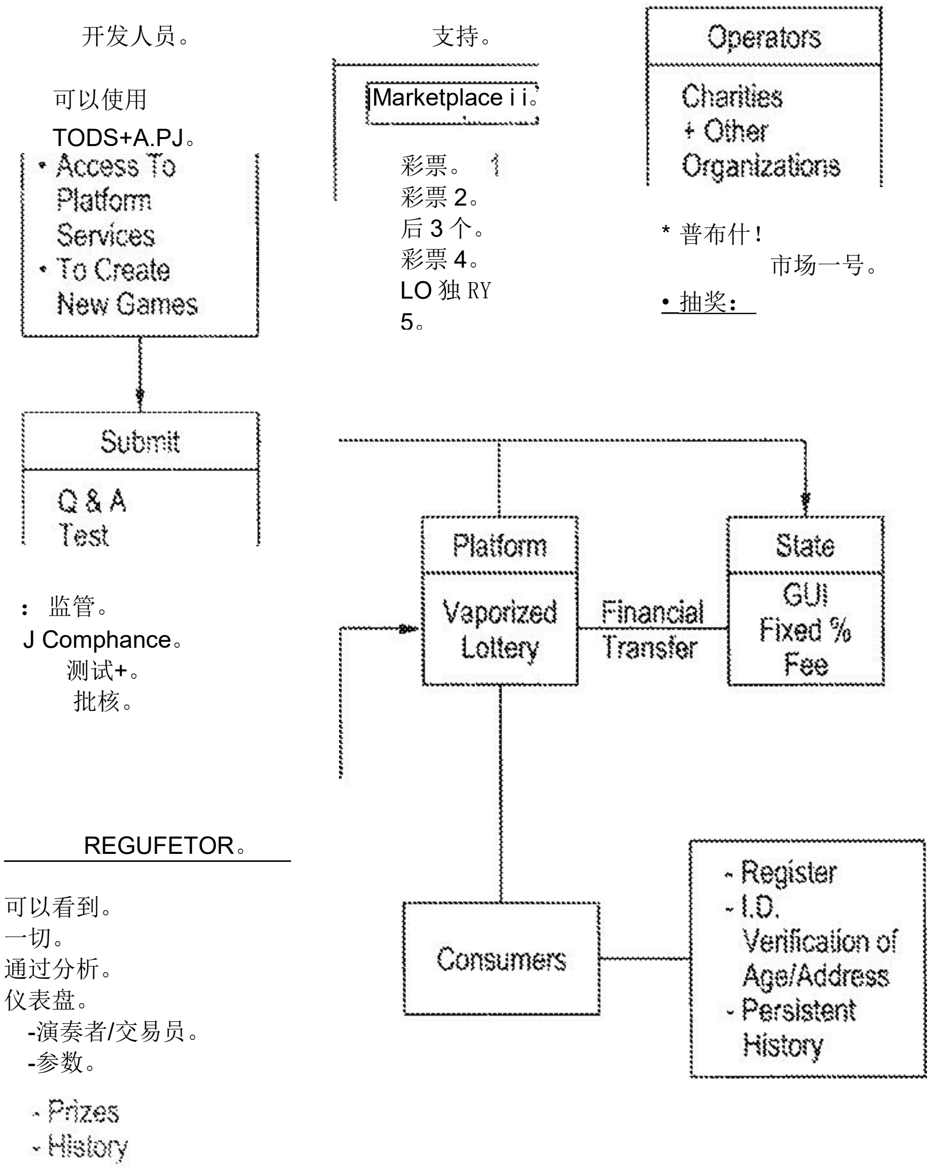
Programmatically Defined Gaming System



Application Plane Layer Explosion

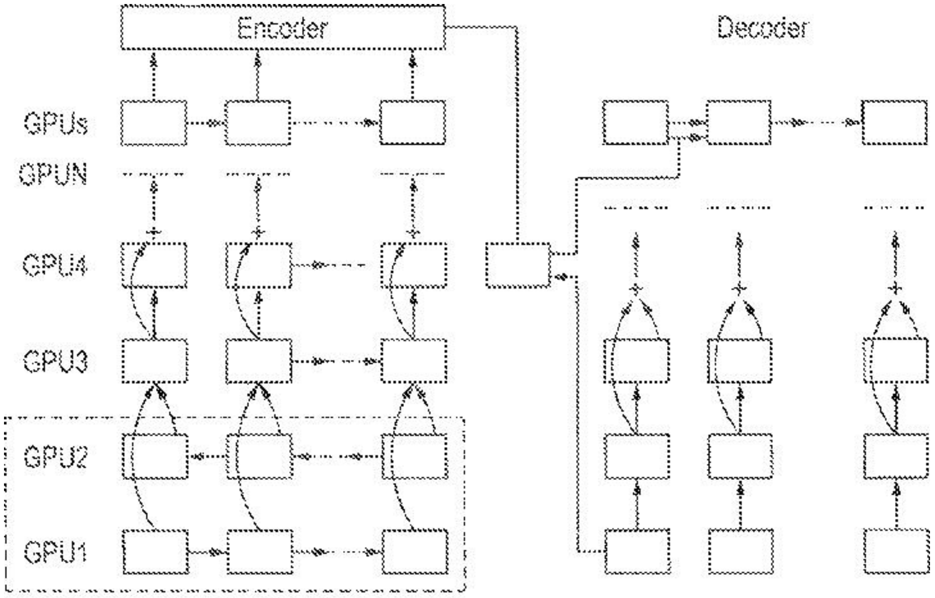

ACI
Interface
Application Interface
Application Interface
Application Interface
Cognitive Computing
AI Unit
Machine Learning
Analytics
SD-ESS Control Logic
Processor
Storage
CSDPI Driver
CSDPI Driver
CSDI
CSDI


CSDI Interface
Management & Control Network Element
Controller
Value/Title Transfer Network Element
I/O Controller
Processor
Output Port
Input Port
CSDI Interface
Entertainment State Network Element
I/O Controller
State Processor
GUI Generator
Input Port
Output Port
Display Driver
Display
Input Devices
IoT Input
External Data



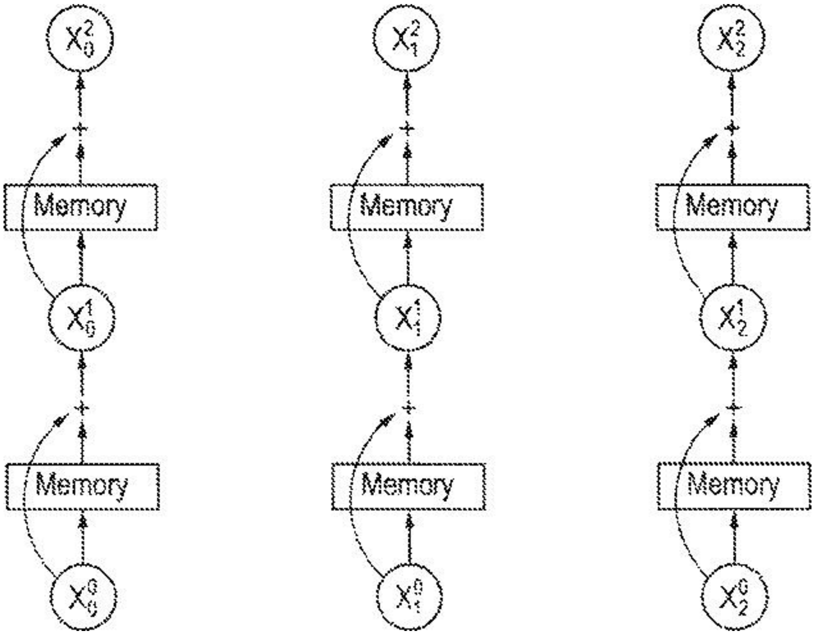
生态系统bHerfacss和hiterConnscthns。

RF«s/。



Neural Network Model Architecture

FIG. 8



神经网络。

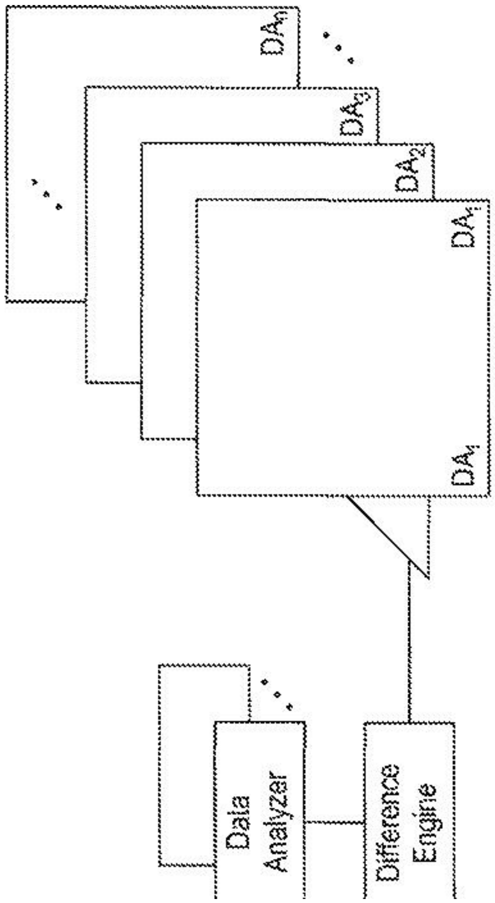


FIG. 10

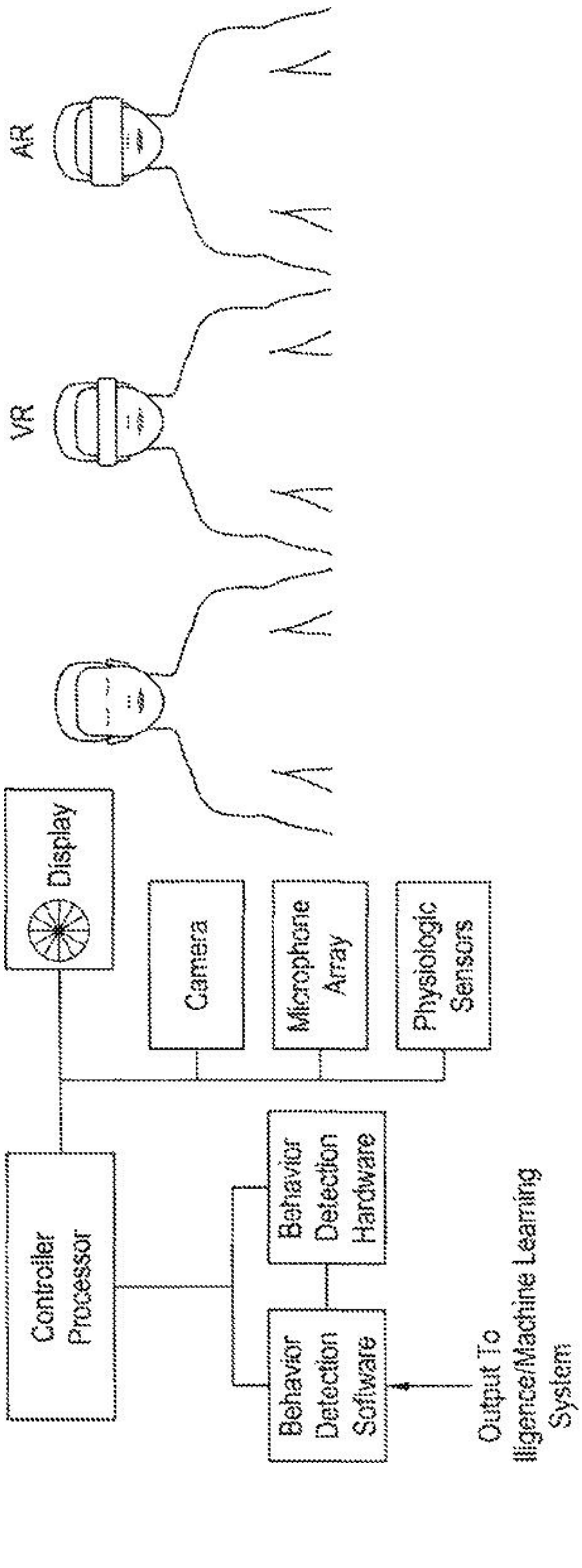
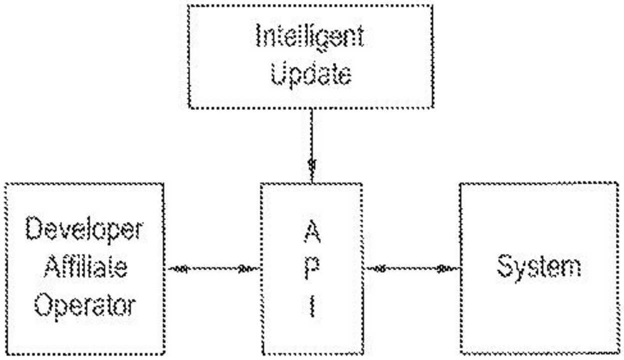
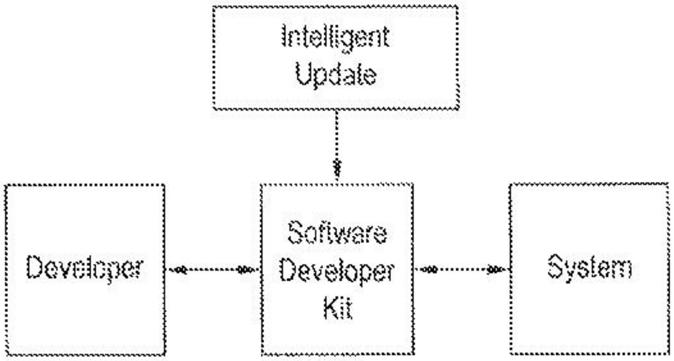

AR
VR
Display
Camera
Microphone Array
Physiologic Sensors
Controller Processor
Behavior Detection Hardware
Behavior Detection Software
Output To lligence/Machine Learning System

FIG. 11



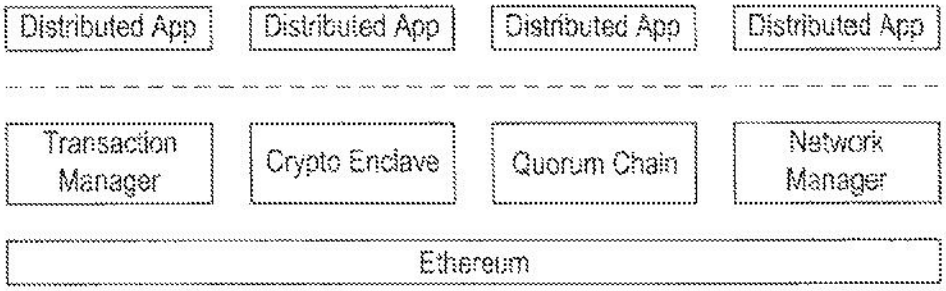
Dynamic Systems d-API

FIG. 12



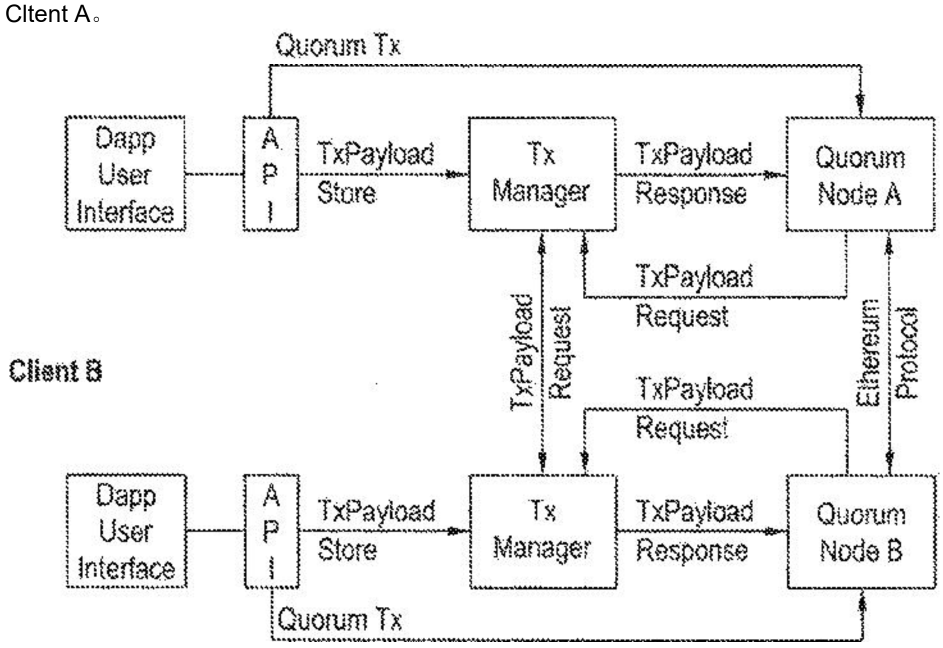
Dynamic Systems d-SDK

FIG. 13



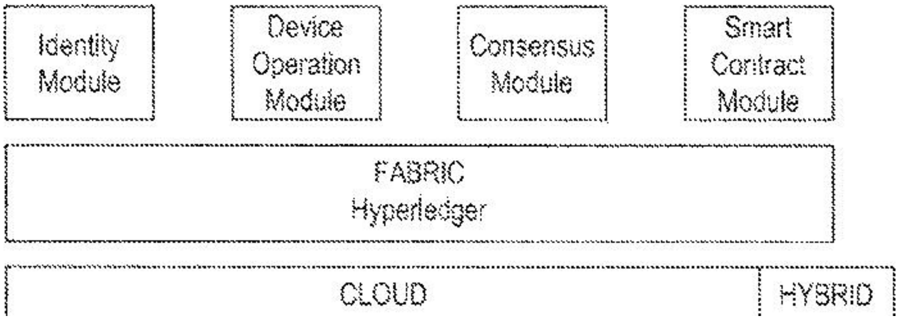
Architecture

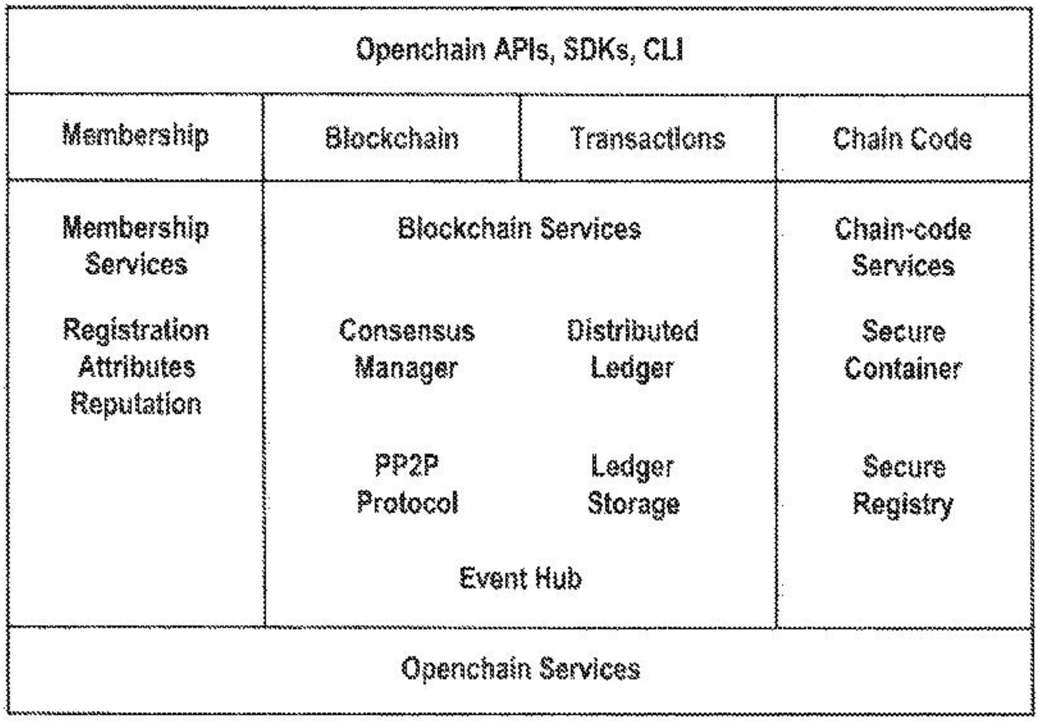
FIG. 14



许可系统。

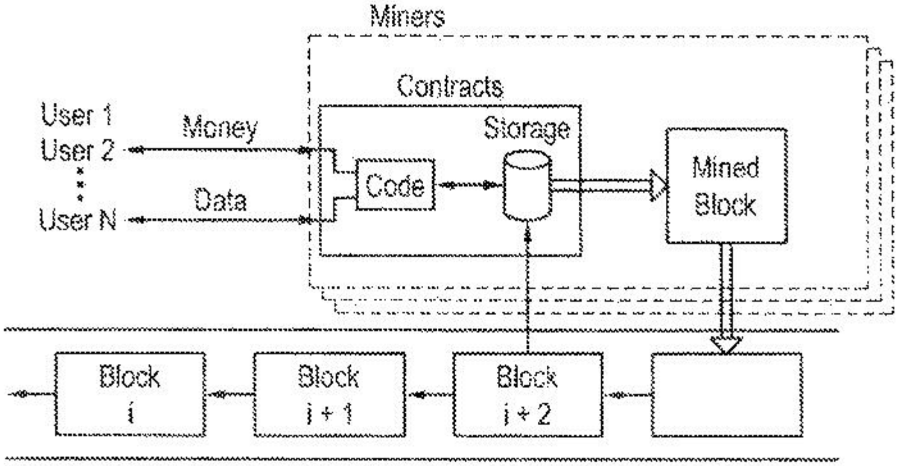
R ‘fUx 第一季度。



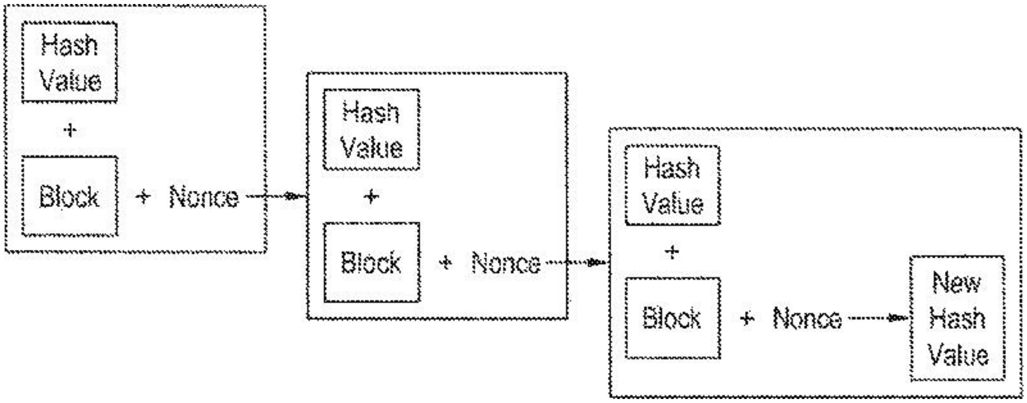


Platform

FIG. 17

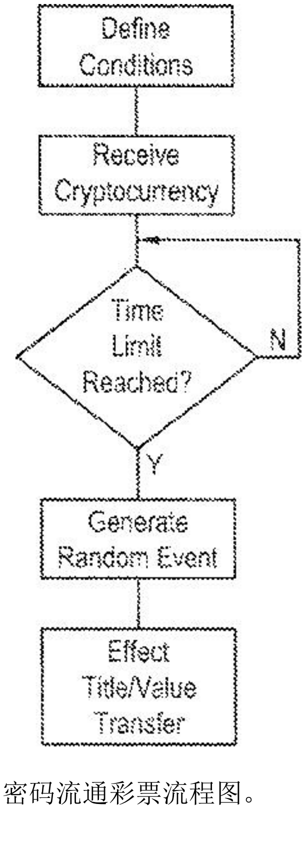


Schematic of a Decentralized Cryptocurrency System with Smart Contracts



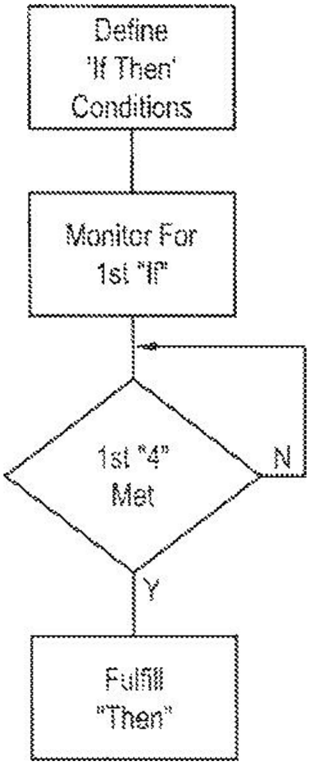
一种创建 S-辱尊龄龄苦熟哈希的模式。
(ha^h Value 瓣游 Block 枷忘源溯曙 New Ha^h 独嫡)。

灯座«10。



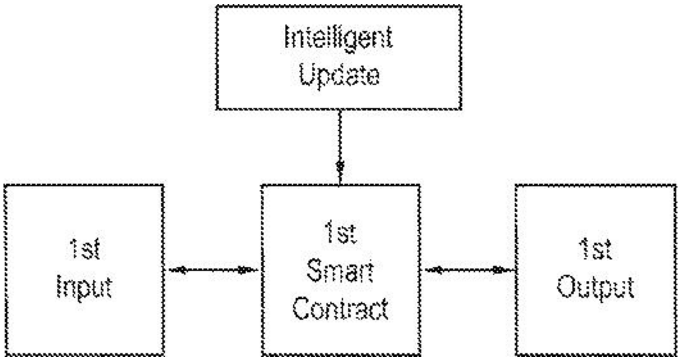
密码流通彩票流程图。

插图。20



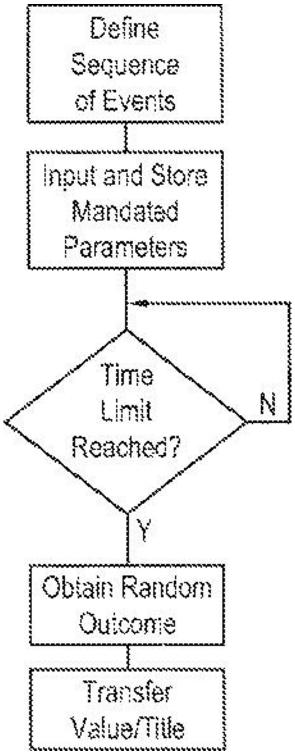
智能契约。

Z f。



Smart-Smart (Smart^2) Contracts

ZZ。



采用强制 VsriaMe 的智能控制。

F/G。23

………顷就 1 英寸荔 F|。…………………………………………………………………………

恣的帐户。

乙醚 4：328.467。

钱币。

支点。

拉亚基。

频率，频率。

广播时间。

最新的 TRansaotsoris。

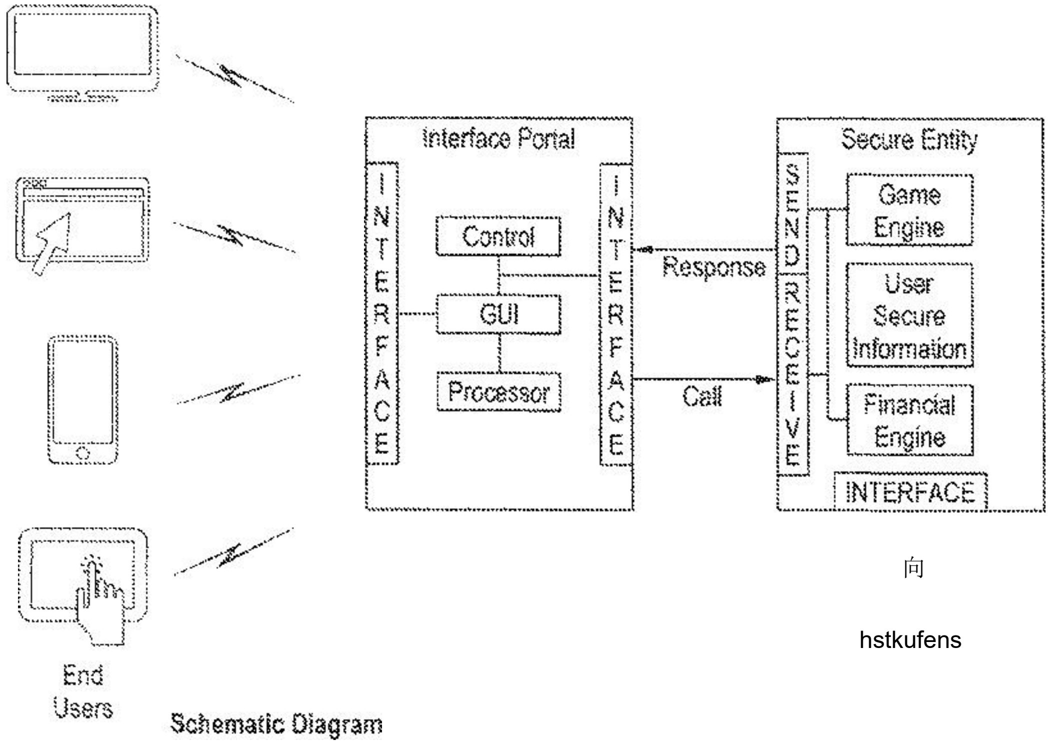
Apd § 12T 怂沁诲 Bewsen Waifets 10Cok？s。

30 加元 0.37 加元。

2 月 2 日奖励庞菲 1160.7 分。

加密并发 WsHef。

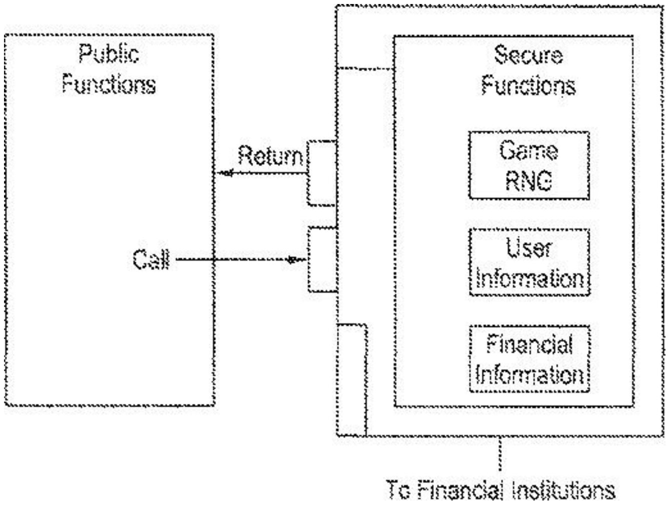
插图。24

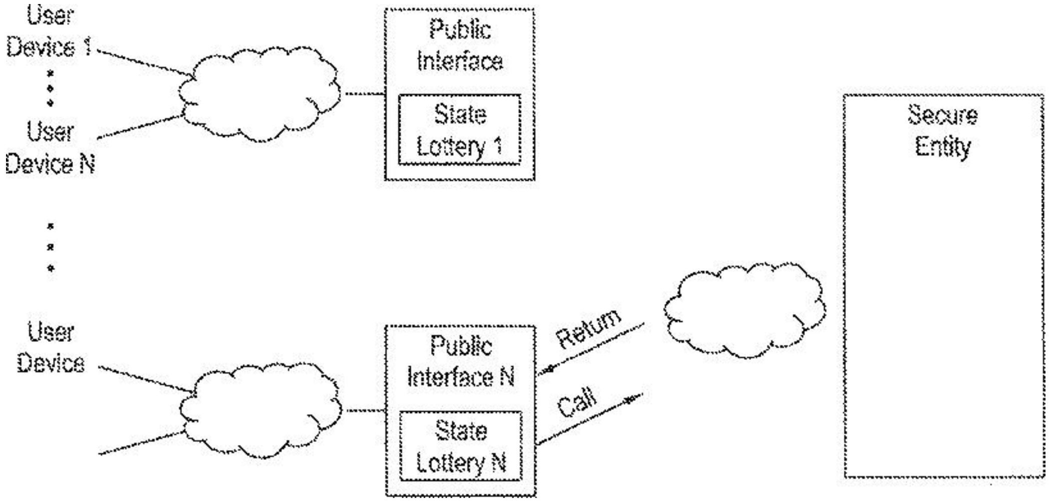


向

hstkufens

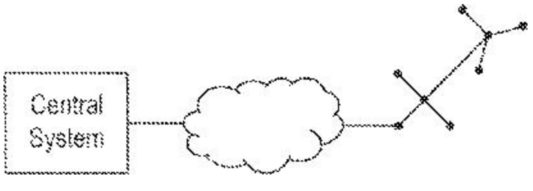
Schematic Diagram





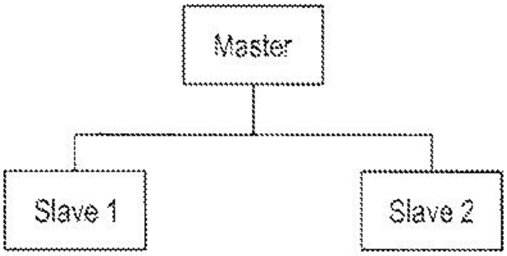
Network Implementation of Segregated Secure and Public Functions

FIG. 27



集中式率系统。

插图。28



Hierarchical Systems

FIG. 29

R)。

J First USA 彩票|。

我约瑟夫・A・斯尼特：

|#。

07/21。

[J]。

彩票信用卡。

图 30。

用于程序定义交易系统和分散加密货币系统的体系结构、系统和方法。

优先权申请。

[0001]这是申请序列号的延续。其要求 2017 年 2 月 3 日提交的临时申请第 62/454,423 号的权益，该临时申请通过引用结合于此，就好像在此完全阐述一样。

本发明的领域。

[0002]本发明涉及用于以编程方式控制的娱乐状态系统的体系结构、系统和方法。更具体地，涉及利用认知计算进行程序控制的体系结构、系统和方法，包括但不限于人工智能和机器学习，并且可选地包括分析。提供了系统、方法和体系结构，利用可选地在对等系统中的包括区块链的分散系统来提供 FBR 游戏和娱乐操作。更具体地说，涉及在分散系统中利用诸如比特币的加密货币实现彩票、游戏或娱乐的系统和方法。

发明背景。

[0003]历史表明，为了提供社会和企业的 FBR 高效运作，许多可信系统已经发展。一般来说，这些都涉及对系统的集中控制，以确保遵守规则。在游戏领域，例子包括彩票和受监管的游戏。例如，内华达州博彩管理委员会监督该州博彩管理机构遵守法律法规的情况，并确保该行业公平和高效地运作。

[0004]考虑一下娱乐和游戏系统背景。彩票是一种“国家”功能，是一种“信任代理”。彩票要素的经典定义是奖金、机会和对价。当这些元素按更正确的时间顺序重新排序时，即首先，收到并持有对价(例如，购票)、机会(例如，确保公平和准确的随机数生成器)和奖品(即，将奖金支付给真正的获胜者)。因此，国家充当一个“信托代理人”，因为它持有对价，保证“4 次机会”的随机性，并支付奖金(所有权转让)。“信任”是建立在系统运营者和监管机构的诚信和可信度的基础上的。彩票或州监管机构往往是前执法人员。对监管机构的信任程度通常基于时间和过往记录，例如，内华达州监管系统被认为是高度值得信赖和有效的，部分是基于数十年的过往记录。此外，在监管过程中失去信任最容易造成企业损失的州最有动力提供监管。这样的系统基于对系统的集中控制。

[0005]赌场是一种四国管制的功能，是一种经过验证的“委托代理”形式。它们由国家颁发许可证，并接受国家检查。

[0006]在游戏和娱乐环境中取得了各种进步。以下内容转让给本协议的受让人，并以引用的方式并入本文中，如同在此完整阐述：游戏，以及在机会游戏和技能游戏中改进游戏的方法，美国帕特。第 6,565,084 号，游戏，以及 FBR 在机会游戏中的方法和设备，美国 PAT。第 6,488,280 号，游戏，以及 FBR 在机会游戏中的方法和设备，美国 PAT。编号 6,811,484， 设备和方法 FBR Game play in a Electronic Environment，U.S.PAT。编号 8,393,946，设备、系统和方法 FBR Implementing Enhanced Gaming and Priking PaRameters in a Electronic Environment(在电子环境中实现增强型游戏和奖励参数的 FBR)，美国专利。编号 7,798,896，设备、系统和方法 FBR Implementing Enhanced Gaming and Priking PaRameters in a Electronic Environment(在电子环境中实施增强型游戏和奖励参数的 FBR)，美国专利。编号 8,241,110，方法和设备 FBR 增强彩票和游戏环境中的游戏，美国专利。编号 8,727,853，方法和设备 FBR Enhanced InteRactive Game Play in Lotting and Gaming Environment， U.S.PAT 。No.8,241,100，Method and System FBR Electronic InteRaction in a Multi-Player Gaming System(多玩家游戏系统中的 FBR 电子交互)，美国专利。8,535,134 号。通常，它们由一套工具组成，以使系统更具吸引力，并优化结果。

[0007]大型系统中的一个令人烦恼的问题是系统不兼容。各种组件通常来自不同的供应商。通常缺乏互操作性和不兼容性。游戏生态系统中的各种系统需要互操作，包括但不限于：游戏运营、营销、CRM(客户关系管理)、忠诚度计划、辅助积分或积分、系统分析和优化以及账户和审计功能。

[0008]软件定义系统是在更高级别的软件控制下互操作的模块集合。它们通过抽象较低级别的功能来管理网络服务。一般来说，存在应用平面、控制平面和数据平面。示例包括具有控制平面的软件定义网络，该控制平面提供对由相对较不智能的交换机、路由器、存储器组成的数据平面的智能控制。另一个例子是软件定义的无线电。控制平面监视和监督数据平面中频段的使用。

[0009]另一个组件是使用静态接口和工具。例如，API 或应用编程接口通常包括静态接口。它们定义了信息请求的格式 FBR。“如果你以特定的方式询问 FBR X，我们会提供 Y‘。一般情况下，除了通过 API，请求者不会提供对系统的访问。还有一个系统是 SDK，即软件开发工具包(Software Development Kit)。它们可能是静态的。提供了实现预期结果的工具。GDK 或游戏开发工具包也可以是静态的，并提供 FBR 游戏开发工具。

[0010]娱乐或游戏的设计通常由度量驱动的设计驱动。这通常涉及 A/B 测试，比较多个系统之间的结果或优惠度。此外，他们经常监测多变量反应系统。

[0011]彩票和乐透风格游戏的一个方面是它们往往是静态的。在最极端的例子中，它们是字面上印在纸板上的。更一般地，一旦选择了一种格式的 FBR 彩票游戏，比如 49 个中的 6 个。

格式，很难更改。公众对变化的看法是，这个游戏对玩家变得不那么有利了。

[0012]赌博问题一直困扰着博彩业。这对社会来说是一个重大问题。虽然用户可以寻求帮助(例如，1-800-Gamling)，但通常会有拒绝和不愿意寻求帮助的情况。已经进行了各种尝试来限制滥用，例如在一些在线游戏中使用速率限制。

[0013]在从实体领域向在线和网络领域转移的过程中，身份问题激增。问题包括：你是你声称的那个人吗？用户的身份会被泄露吗？

[0014]认知智能和适应性智能取得了重大进展。例如，IBM Watson 在 2011 年与高技能选手举行的"危险边缘"(Jeopardy)比赛中获胜。深度学习和模式识别已经出现。目前的趋势包括大数据、模式识别和机器学习。

[0015]在 2D 和 3D 空间中的目标检测方面也取得了最新进展。大规模视觉识别挑战赛(LSVRC)中的一项挑战在 ImageNet 2016 中提供了 FBR 对象检测。ImageNet 的自动标签错误率降至不到 3%，而人工操作的错误率约为 5%。

[0016]在基于机器的游戏性能方面也取得了重大进展。2015 年，Google Deep Mind 使用人工智能强化学习系统学习如何玩 49 款雅达利游戏。2016 年，谷歌的 AlphaGo 系统以 4：1 击败了世界上最伟大的围棋选手之一。2017 年，卡内基梅隆大学(Carnegie Mellon University)的 LiBRatus 项目以统计意义上的方式击败了顶级人类选手。

[0017]在基于云的系统方面取得了进一步的进展。功能已经从本地服务器和存储迁移到远程"云"存储。这些系统提供了 FBR 轻松的可扩展性。基于云的系统可以同时运行多个 4 个实例。他们还可以结合软件即服务，包括人工智能("Al")。

[0018]物联网(IoT)利用能够向远程位置发送数据和接收命令数据的设备。各种语音控制设备使用人工智能或机器学习(ML)，例如 AmAzon Alexa、Google Dot。**[0019]图 1.。1** 示出了示例性的现有技术集中系统。插图。**2** 示出了示例性的现有技术分布式系统。

[0020]在可信分布式系统中取得了进步，例如在使用基于区块链的系统方面。区块链技术的最初披露归功于中本聪(Satoshi Nakamoto)在 2008 年 10 月发表的一篇论文。该系统提供 FBR 自动信任或系统信任。区块链范式为 FBR 提供了一个利用分散共识的分散系统。这可以在没有中介的情况下以点对点的方式完成。该系统可以被视为在可编程分布式网络上运行软件的节点网络。它有时被称为具有共享状态事务单例机器、基于事务的状态机、消息传递框架、可信对象消息传递计算框架和可信计算。

[0021]区块链和密码学的结合建立了分散共识。权威和信任由分散的虚拟网络提供。共识。逻辑通常与应用程序分开。它可以包括分散架构的第一层。

[0022]区块链使用分布式分类帐。"块"由一组新的已接受事务组成。一批交易在一块中被释放，以由参与计算机的网络进行验证。公共区块上连续的、顺序的交易记录创建了唯一的"链"或区块链。此块将发布到所有其他节点。该出版物定期发布，例如每 10 分钟发布一次。

[0023]EtheriUm 是一个开源的 FBR 智能合约平台。就目前的运营而言，EtheriUm 是一个运行智能合同的去中心化平台：应用程序完全按照程序运行，没有任何停机、审查、欺诈或第三方干扰的可能性。这些应用程序运行在定制的区块链上，这是一种极其强大的共享全球基础设施，可以移动价值并代表财产的所有权。这允许开发商根据长期的指示(如遗嘱或期货合约)创建市场、存储债务或承诺记录、转移资金，而不存在交易对手风险。EtheriUm 还表示，其目标是创建一种可交易的数字令牌，可以用作货币、资产的表示、虚拟份额、成员资格证明或任何东西。这些代币使用标准的硬币 API，因此合同将自动与任何钱包、也使用此标准的其他合同或交易所兼容。流通中的令牌总量可以设置为简单的固定量，也可以根据任何编程规则集进行浮动。总而言之，EtheriUm 表示，它可以建立一个固定供应的可交易令牌，一个可以发行货币的中央银行，以及一种基于谜题的加密货币。

[0024]当前的系统有许多缺点。他们改变和创新的速度很慢。它们通常涉及不能互操作的专有系统。这往往存在政府和/或体制上的偏见。可能会有一个繁琐的监管环境。最后，交易成本往往很高。

[0025]因此，需要在不一致的、通常是专有的系统之间进行 FBR 互操作性。有必要在更全球化的基础上限制 FBR 赌博，包括地理模拟和全球使用率监测 FBR 问题赌博。有必要对 FBR 问题进行赌博检测和补救。因此，需要对分布式系统进行 FBR 改进。

发明内容。

[0026]在一个方面，本发明包括使用分布式分类账的交易状态系统的系统 FBR 控制。首先，该系统包括适于接收关于事务状态系统的操作的指令的应用平面层。优选地，应用平面层耦合到应用平面层接口。第二，提供控制平面层，该控制平面层包括自适应控制单元，诸如认知计算单元、人工智能单元或机器学习单元。第三，数据平面层包括输入接口，以接收来自一个或多个数据源的数据输入，并提供耦合到分散分布式分类帐的输出，数据平面层耦合到控制平面层。可选地，分散的分布式分类帐存储关于加密货币的数据。

[0027]提供了 FBR 训练人工智能系统的系统和方法，该系统和方法包括使用一个或多个人类主体对刺激的反应作为。

人工智能系统。一个或多个显示器朝向人类受试者以向人类受试者呈现刺激。一个或多个检测器用于监视人类受试者对刺激的反应，所述检测器至少包括运动检测器，所述检测器提供输出。耦合分析系统以接收检测器的输出，该分析系统提供对应于人类受试者的反应是阳性还是阴性的输出。当分析系统的输出为正时，神经网络利用分析系统的输出为神经网络的训练提供正权重，当分析系统的输出为负时，神经网络为神经网络的训练提供负权重。

附图的简要说明。

[0028]图 3.。1 是现有技术集中式系统的示意图。

[0029]图 3.。2 是现有技术集中系统的示意图。

[0030]图 3.。3 是显示应用平面、控制平面和状态数据平面的程序定义娱乐状态系统(PD-ESS)的系统级框图。

[0031]图 3.。4 是 PD-ESS 的应用状态平面层的系统级框图爆炸。

[0032]图 3.。5 是 PD-ESS 控制平面层的系统级框图爆炸。

[0033]图 3.。6 是 PD-ESS 的状态数据平面层的系统级框图爆炸。

[0034]图 3.。7 是生态系统的图解视图，包括接口和互连。

[0035]图 3.。8 是包括图形处理单元(GPU)的神经网络模型体系结构的系统级框图。

[0036]图 3.。9 是神经网络模型体系结构的系统级框图。

[0037]图 3.。10 是包括差异引擎和数据分析器的多个数据集的系统级图。

[0038]图 3.。11 是响应系统显示和检测系统，用于生成训练人工智能(AI)和机器学习(ML)系统的输入。

[0039]图 3.12 是动态系统应用编程接口(D-API)的系统级图。

[0040]图 4.。13 是动态软件开发工具包(d-SDK)的系统级图。

[0041]图 4.。14 是包括区块链和以太网的分布式系统的系统架构层级图。

[0042]图 4.。15 是允许的区块链系统的系统架构层级图。

[0043]图 3.。16 是区块链平台的系统架构层级图。

[0044]图 3.。17 是包含开链服务的区块链平台的系统架构层级图。

[0045]图 3.。18 是具有智能合约的去中心化加密货币系统的系统架构层级图。[0046]图 4.。19 是具有顺序散列值创建的分散系统的系统体系结构层级图。[0047]图 3.。20 是加密货币彩票的流程图。

[0048]图 3.。21 是智能合约的流程图。[0049]图 3.。22 是智能-智能(Smart2)合同的流程图。

[0050]图 3.。23 是具有强制和可变参数的智能合同的流程图。

[0051]图 3.。24 是加密货币钱包的图形用户界面(GUI)。

[0052]图 3.。25 是具有分离的公共和安全功能的系统的系统体系结构级示意图。

[0053]图 3.。26 是分离的公共和安全功能的接口的系统体系结构级别。

[0054]图 3.。27 是具有分离的公共和安全功能的系统的网络实现的系统体系结构级别。

[0055]图 3.。28 是集中式和分散式相结合的系统架构层。

[0056]图 3.。29 是分层系统的系统架构级别。

[0057]图 3.。30 是彩票关联信用卡的平面图。

本发明的详细描述。

[0058]用于节目定义的娱乐状态系统的体系结构、系统和方法。

[0059]下面的描述主要结合图 6。3、4、5 和 6，但也可适用于其他数字。提供了一种体系结构，该体系结构是节目定义的娱乐状态系统。这优选地用于将控制整体体验的系统与定义状态的底层系统分离。第一平面即应用平面提供接口，主要是 FBR 系统侧用户，例如事件、竞赛、彩票的组织者、开发者。第二个平面，控制平面，提供 FBR 智能控制，特别是认知计算，包括人工智能和/或机器学习，包括系统随着时间学习的人工智能。这优选地在模块之上提供智能控制层。第三平面，即状态数据平面，为 FBR 娱乐 4 状^{态}模块提供各种机制，优选地包括“核心环路”、元状态，并提供接口 FBR 终端用户以及输入和输出。

[0060]图 3.。3 提供了框图程序定义的娱乐状态系统(PD-ESS)。插图。4 是 PD-ESS 应用平面层的爆炸式增长，包括应用层 GUI(面向开发人员、分支机构和慈善机构)。插图。5 提供爆炸 PD-ESS 控制器平面层。插图。6 提供爆炸 PD-ESS 状态数据平面层。还包括娱乐状态网元层的爆炸性增长、用户界面 GUI、价值/所有权转移网元的爆炸性增长以及其他功能块的爆炸性增长。

[0061]首先转到应用平面层，程序用于向 PD-ESS 控制器传达要求和期望的行为。它通过 PD-ESS 应用控制器接口(ACI)提供 PD-ESS 应用和 PD-ESS 控制器之间的通信。可选地提供应用程序逻辑和驱动程序。应用层可以接收状态数据平面动作的抽象视图。PD-ESS 应用程序可以与更高级别的抽象控制接口。该系统包括一个接口，即 PD-ESS 应用控制器接口(ACI)。优选地，该管理和管理提供以下内容：(1)到/从应用平面，它提供合同和 SLA，(2)到/从控制。

平面配置策略、监视性能和(3)数据平面元素设置。

[0062]第二转到控制平面层，PD-ESS 控制器在理想的逻辑上是集中式实体，优选地用于将 PD-ESS 应用的要求转换到状态数据平面层，并向应用层提供状态数据平面中的动作(例如，事件信息和统计信息)。控制平面可以从数据平面向应用平面提供统计数据、事件和状态。控制平面优选地在数据平面中的低级控制处实施行为，提供能力发现，并监视统计数据和故障。控制平面有利地包括认知计算，诸如人工智能(Al)和机器学习(ML)，下面将更详细地描述。

[0063]控制平面可以可选地包括分析，包括但不限于模式识别。可以对群体(最好是相关群体)或子集执行分析。优选地，该子集具有与目标用户相似的特征。数据可以根据子集入库。可以分析原始数据的范围。可以包括预测建模。可以在控制平面级别实施负责任的游戏控制，特别是在存在使用率限制和全局限制的情况下。

[0064]第三，转向状态数据平面层，其优选地包括主要子组件和功能网元。可选地，功能网元包括以下部分或全部：1.。娱乐状态网元，2.。价值/所有权转让网元，3.。游戏库，如赌场，VET，电子游戏，锦标赛，有奖游乐设施(AWP)，游戏机制，核心循环，技能，揭秘技能，第二次机会，社交，游戏化，奖品，vGLEP 和奖牌，4.。系统、市场营销、促销、CRM、运营、物流、互动、移动/应用程序和响应性设计，5.。站台，6.。频道，7。彩票，包括零售和中央系统，8。忠诚度，9.。负责任的游戏控制，可选地包括使用速率限制和全局限制(也可以在控制平面层中进行)，10.。体育，包括现实世界、梦幻和电子竞技，11 分。Other Live Data Entertainment，12。网络，包括网络通信和网络服务以及 13。管理，包括记录、玩家账户管理、报告、合规性(包括法规遵从性)、安全(包括网络安全、欺诈和风险管理，最好包括审计和支付)。

[0065]娱乐状态网元提供与系统用户的接口 FBR 交互。输入从用户选择接收信息。传感器可以是各种形式，包括声音传感器、运动传感器，无论是 2-D 还是 3-D，例如包括微软 Kinect 系统。“内部数据”主要由与游戏操作相关的数据组成。“要与主数据源组合的 ExtemaF 数据源。这些可能包括 1 个。位置，2。当前活动，如驾驶(由车辆提供，由跟踪电话提供)或锻炼(由 FitBit 或类似工具提供)，3.。经济状况，4.。天气，5。最近的事件/新闻，例如，最近的一次大型强力球胜利，6.。营销信息，7.电子邮件扫描，例如，谷歌扫描 Gmail FBR 内容，8.。社交媒体，以及 9.物联网(LOT)。物联网(LOT)提供了各种形式的互联设备，如数据传感器。传感器产生数据输入“刺激”到系统。通过利用任何形式的输入，该系统能够提供 FBR 大规模并行性。对系统的所有数据“刺激”允许系统对所有数据刺激进行自适应和反应。

[0066]输出为用户提供刺激。表单可能包括：1.图像，例如在显示器上，或通过 GUI 或 VR 系统、AR 系统，2.。具有远程计算能力的瘦客户机显示器，3.。投影和全息图，4.声音，5.触觉刺激，6.嗅觉刺激，或 7.神经或其他直接电刺激。

[0067]价值/所有权转移网元用于接收和转移价值(货币、硬币和其他有价物品)。价值可以指可替代的流动资产或其他价值储存。所有权一般指不动产、动产或虚拟财产的所有权。下面详细讨论了区块链、无信任和加密货币系统。

[0068]人工智能(AI)广泛地说是计算机科学中处理智能行为自动化分支。它们是系统，其目标是使用机器来模拟和模拟人类的智能和相应的行为。这可以采取多种形式，包括符号或符号操作 Al。它可以解决分析抽象符号和/或人类可读符号的问题。它可以在数据或其他信息或刺激之间形成抽象连接。它可能会形成合乎逻辑的结论。人工智能是机器、程序或软件所展示的智能。它被定义为智能 Agent 的研究和设计，其中智能 Agent 是一个感知环境并采取行动最大化成功机会的系统。还有一些人将其定义为制造智能机器的科学和工程。

[0069]人工智能通常涉及到神经网络的使用。在各种实施例中，使用神经网络节点的多层堆栈。最低层由颗粒状元素组成。作为游戏应用中的示例，按照更高级别理解的顺序，级别将从单个动作的实例(粒度)、核心循环检测、会话播放、到多会话播放进行。可选地，解析引擎用于将较大的集合(例如数据集或图像)分解或细分为更离散或更细粒度的元素。

[0070]Al 可以具有各种属性。它可能有演绎、推理和问题解决。它可能包括知识表示或学习。系统可以执行自然语言处理(通信)。还有一些人执行感知、运动检测和信息处理。在更高的抽象层次上，它可能会产生社交智力、创造力和一般智力。采用了多种方法，包括控制论和脑模拟、符号、次符号和统计学，以及整合这些方法。

[0071]可以单独或组合使用各种工具。它们包括搜索和优化、逻辑学、概率方法、FBR 不确定性推理、分类器和统计学习方法、神经网络、深度前馈神经网络、深度递归神经网络、深度学习、控制理论和语言。

[0072]Al 有利地在其体系结构中利用并行处理，甚至大规模并行处理。图形处理单元(GPU)提供 FBR 并行处理。当前版本的 GPU 可从各种来源获得，例如 NVIDIA、Nervana Systems。

[0073]机器学习被定义为从经验中构建知识的系统。机器学习用于发现模式和规律。

[0074]深度学习使用神经智能。它易于扩展，通常涉及更多层或神经网络(NN)。神经网络可以有多种形式，包括：有效神经网络、矢量化神经网络、矢量化 Logistic 回归、矢量化 Logistic 回归梯度输出、二分类、Logistic 回归、Logistic 回归代价函数、梯度下降、导数、计算图和 Logistic 回归梯度下降。

[0075]深度神经网络(DNN)通常涉及超参数调整。通常，它们利用正则化和最优化。有时它们被称为深度信念网络(DBN)。

[0076]其他形式的神经网络包括卷积神经网络(CNN)或递归神经网络(RNN)。可用系统的示例包括：LSTM、Adam、Caffe、Dropout、Batch Norm、Xavier/He、Python、Scikit-Leam 和 TensorFlow。

[0077]A1 可以对各种形式的数据集进行操作。数据集可以包括图像，无论是视频图像、2D 数据和/或 3D 数据。可以分析顺序数据。示例包括但不限于自然语言、音频、自动驾驶决策、游戏状态和游戏决策。

[0078]各种工业应用有利地受益于铝的应用。它们包括成像和目标检测，用于识别、分类、挖掘和可选地提供情感分析。其他应用包括自动驾驶。然而，其他应用包括机器人和机器人技术。在医疗保健领域，功能包括成像分析、诊断和游戏化。可以增强各种形式的顺序数据分析，例如语音识别和自然语言处理。音乐应用包括识别和合成。在游戏领域内，应用包括游戏状态序列检测、分析、编队、组合优化和游戏优化。聊天机器人和机器翻译有利地使用了这些系统。

[0079]图 3.。**7** 显示了娱乐或游戏生态系统内的组成功能块。附属公司的作用是获得客户。附属公司收取佣金，例如根据获得的用户数量或收入的百分比(%)。可选地，存在到信用卡功能的链接(将在下面结合图进行讨论。**30)。**

[0080]接下来是计划举办彩票、游戏或其他娱乐活动的慈善机构和其他组织。他们提供客户获取服务。他们是活动(游戏、彩票或娱乐)的接受者。他们还收取费用。

[0081]接下来是开发人员，他们提供游戏设计。作为游戏设计的回报，他们获得了多司法管辖区的使用和付费 FBR 的使用。可以提供增强的应用或应用商店，其中可以查看、选择和下载游戏设计。

[0082]接下来，消费者提供注册和标识信息。注册数据可以可选地包括身份、年龄、地址和验证。可选)数据足以使系统符合了解您的客户(KYC)规则，可选级别为实名认证。这将存储为永久历史记录。客户获得了玩、赢和接受娱乐的机会。

[0083]接下来是监管机构或信任验证代理。他们提供测试、审批、FBR 游戏公平、整体审批，确保合规和安全。系统授予监管者或信任验证代理对每笔交易(分析仪表板)、玩家帐户、参数、奖金金额和支付以及完整历史记录的访问权限。监管机构或信托验证代理机构获得补偿，无论是费用还是交易金额的一定比例。**[0084]接**下来，彩票充当信托代理，并收取交易额的一定比例。可选地，当彩票的历史功能由生态系统内的另一实体执行时，这些功能可以从系统中消除或蒸发。

[0085]无花果。8 和 **9** 涉及 FBR 训练神经网络的学习过程。通过提供重复的输入刺激，然后训练神经网络以提供正确的输出，可以教导系统基于一个或多个输入刺激形成正确的关联输出。在将输入转换为期望输出时，训练可以包括监督学习，例如当目标值和参数被监督时。或者，训练可以是非监督学习，其中系统试图识别输入中具有可识别结构并且可以再现的模式。或者，系统可以使用强化学习，它独立工作(类似于无监督学习)，但根据成功或失败来奖励或惩罚。优选地，强化学习涉及增量改变。在各种训练技术中，可以使用扰动，其中一个或多个输入参数通常以例如小于输入值的 10%、更优选地小于 5%和更优选地小于 3%的扰动量变化，以便监视扰动对输出的影响。在各种训练技术中，可以使用扰动，其中一个或多个输入参数通常以小于输入值的 10%、更优选地小于 5%和更优选地小于 3%的扰动量变化，以便监视扰动对输出的影响。

[0086]超参数和参数可以在 AI 或机器学习系统中使用。模型参数是根据数据自动估计的。可以根据数据估计模型内部的配置变量。这可能是模型在进行预测时所要求的。值定义了模型的技能。它们可以通过数据进行估计或学习。

[0087]超级参数是手动设置的，并在流程中用于帮助估计参数。使用模型外部的配置变量。一般来说，它不能从数据中估计出来。它们经常用于估计模型参数的过程中。它们通常由系统用户指定。通常可以使用试探法设置超参数。它们经常被调整为 FBR，这是一个给定的预测建模问题。超级分类帐可以用作超级分类帐编写器或超级分类帐结构。

[0088]可以在各种类型的硬件上执行人工智能或机器学习。有利的是，支持并行处理的系统可以提供 FBR 计算速度和效率。NVIDIA 和 AMD 提供图形处理单元(GPU)等并行处理单元。麒麟 970 提供神经处理单元(NPU)。Apple All 和高通第零度处理器。人工智能和机器学习处理也可以作为云人工智能或机器学习系统提供，如 Google 和 AmAzon Web Services 提供的。

[0089]图 3.。10 描述了域转换和差异引擎。一个有利的域变换涉及时域到频域(时间序列到频域)。傅立叶级数就是一个例子，它通常用于重复信号，例如振荡系统。傅立叶变换通常用于非重复信号，例如瞬变信号。可以使用诸如快速傅立叶变换(FFT)之类的增强计算技术来提高 FBR 效率和计算速度。另一种域变换是拉普拉斯变换，通常用于电子电路和控制系统。另一种是 Z 变换，通常用于离散时间信号。可以有利地使用数字信号处理器(DSP)。谱密度估计可能包括小波分析、图像分析、数据压缩和多变量分析。有利地使用相关数据集。

[0090]可以使用区分引擎来识别两组或更多组数据之间的区别。该差别可以是基于时间的，例如其中一个数据集与时间 0 有关，而另一组与时间 1、时间 2、时间 3、…、时间 **N** 有关。可以计算图像中的差别。

[0091]图 3.。11 示出了一个系统，在该系统中，可以监视、捕获和分析受试者的反应，然后将其用作 A1 的输入。在各种努力中，例如在游戏或娱乐设计和创作中，可以监视、分析和使用目标受众的反应来训练人工智能或机器学习系统。受试者对娱乐/游戏刺激的反应用来测量受试者所经历的‘乐趣’，然后该测量(‘FIM’)被用作 A1 或 ML 系统的训练输入。该系统可以检测个体主体行为。或者，该系统可以监视群体行为，用于检测“有趣”的体验，但也可以测量群体或人群的属性，例如兴奋、参与度或基于群体的行为。

[0092]提供显示器作为对一个或多个对象的刺激。可以使用平板显示器或监视器。可选地，可以利用个人观看设备，诸如单独的屏幕、虚拟现实耳机、增强现实设备、平视显示器、投影设备或成像技术。

[0093]利用各种检测器来监视一个或多个受试者的反应。运动检测利用运动跟踪硬件和软件。一台照相机拍摄被摄体的图像。各种摄像头包括微软 Kinect、2D 传感器和摄像头以及 3D 传感器和摄像头。度量检测器可以分析身体部位的位置，例如肢体、关节或面部特征。它可以测量速度、运动、位置或运动的更高级别的导数，如变化率。面部探测器监控 FBR 面部识别。可以检测面部属性，例如正面属性(例如，微笑)或负面属性(例如，皱眉)。可以确定身体位置检测。声音检测可以用麦克风或麦克风阵列来执行。它可以检测声音的属性，例如正面属性(例如，欢呼声)和负面属性(例如，咒骂和嘘声)。利用生物测定扫描检测。生理反应检测可选择性地监测受试者的心率、血压、瞳孔扩张、体温、心电图和精神活动。活动监控检测器监控参与响应，最好包括下注率、参与时间。显示、保留率、重复率和再参与率。有利地利用了分析。

[0094]系统的输出用作人工智能或机器学习系统的输入。例如，在神经网络中使用强化学习的训练中，正权重使用 FBR 正属性，负权重使用 FBR 负属性。

[0095]该系统还可以提供被识别为与成瘾(例如赌博成瘾)相关联的输出，或者与以其他方式对游戏上瘾的对象相关联的输出。当参与程度或轻微上瘾被视为可接受时，可在训练中使用正权重，而当上瘾被视为不可接受或过度时，可在训练中使用负权重。

[0096]人工智能、机器学习、神经网络、在训练 AI/ML 系统中使用用户响应(通常图 2)。**11** 和上面的讨论)可以有利地用于游戏设计和开发、娱乐开发和/或任何创造性开发工作。

[0097]这些系统可以构成工具矩阵。它们可以包括一组给定的工具。从更根本的意义上说，它们包含了一个发现工具的工具。工具可以是游戏状态、娱乐状态或任何形式的状态或物质。

[0098]下面将描述游戏开发，但是工具、系统、方法和架构可以应用于娱乐或任何创造性工作。对于特定的游戏，第一个选项是只提供该特定游戏的基本规则。为了发现获胜的游戏策略，该系统可以与其自身对战，或者与其他系统对战。在另一种选择中，可以向系统提供已知的游戏比特，允许系统使用或忽略游戏比特。在又一备选实施例中，该系统可以配备有游戏库。该系统可以分析游戏库、FBR 游戏元素、游戏机制或核心循环。可选地，系统可以将游戏库的分析限制为类似的游戏，或者可以考虑可选地分成子单元的所有游戏，例如纸牌游戏、棋盘游戏、视频游戏。一旦定义了各种核心循环或游戏元素，系统就可以将它们组合成各种组合和排列，以便定义新的游戏或游戏进行序列。系统可以识别数据中的模式。可以将值分配给各个点或游戏状态或游戏状态决策点的决策。用户响应的使用可以有利地用于游戏形成和优化。用户响应的使用特别适合于强化学习。

[0099]该系统可以以分层方式操作。可以使用分级系统，其中它可以改变一个从属强制参数，只要满足“上级”或“主”强制参数即可。举例来说，可以使用‘超级’强制参数‘来保证特定的结果。可替换地，可以授予管理控制，诸如设置‘top LeveF 约束’。

[0100]系统可以考虑合作动作中的单独功能。职能可能会被重新分配或转移到其他(特别是较低的)行动级别。系统可能会提供新的变量。通过提供分层响应，可以维护核心功能。可选地，该系统可以例如基于来自管理员的命令或基于预定义的标准来使用系统的“终止开关”FBR、凋亡。该系统可以提供。

体验包(“Total RecalF”)，例如处于连续状态和/或持续状态。

[0101]无花果。12 和 13 涉及各种动态的、多变的系统。在名称“d-API”和“d-SDK”中，‘d’代表 4dynamic‘，并且能够在系统内和由系统进行更改。交互(请求和/或响应)的格式可以是改变。或者，它可以改变响应中提供的信息的类型、数量或质量。其他可能更改的因素包括请求通过 API 或 SDK 更改信息的能力。可以更改其他操作或管理权限，例如只读访问、读写、编辑权限、超级管理权限。这些都提供了自适应控制下的 FBR 动态变化。

[0102]在动态应用编程接口(d-API)内，定义初始格式的 FBR 请求和响应。这可以在 tiSThen，语句中考虑：如果您要求 FBR X 采用商定的格式，则系统将提供 X。动态系统可能会改变格式和/或响应。智能动态更新可以基于人工智能、机器学习或分析。虽然不限于以下，但这些改变中的一些或全部可以动态实现：交互的格式(请求和/或响应)、对更多信息或功能的访问(例如只读)或修改权限、向系统提供信息或数据的能力、以及改变数据的能力。

[0103]在动态游戏开发工具包(d-GDK)中，提供了初始工具包。然后，系统允许动态修改 GDK。优选地，动态修改基于人工智能或机器学习或分析。

[0104]可以提供动态隔离彩票(d-SL)，其中可以提供一个或多个功能单元或彩票。可以使用虚拟化系统，例如在使用虚拟化服务器时。

[0105]无花果。14-20 涉及区块链实现 FBR 游戏、娱乐或其他有用的目的。区块链使用加密的“散列”来识别每个区块和交易。每个连续的块都包含先前代码的散列。这将按时间顺序永久修复事务。区块链同时利用私钥和公钥。将先前的散列与现时值一起添加到新的区块链中，以形成新的散列。

[0106]加密货币提供 FBR 加密安全交易。加密货币是一种可编程货币或分散的价值转移系统。它也是一种去中心化的虚拟货币或去中心化的数字货币。

[0107]工作证明或利害关系证明是参与区块链的“权利”。它必须足够繁重，可以在不重做工作的情况下阻止更改。比特币是一种创造的货币，它被挖掘出来，作为一种奖励，用于 FBR 支付处理工作。区块链加密货币不涉及交易手续费或购买者支付的费用。没有退款权利或退款。

[0108]它可以在任何形式的公共和私有网络中实现。可以使用开放软件和专有软件。存储可以是本地存储或云存储和计算。分析可以在本地或在云分析系统中执行。可以执行分析即服务(AAAS)。系统可以是许可的，而不是无许可的分布式系统。

[0109]无花果。21 至 23 **与**智能合约有关。核心要素是，第一，一套承诺，可以是合同的，也可以是非合同的。其次，它们以数字形式指定，以电子方式运行，其中合同条款或功能成果嵌入代码中。第三，它们包括基于协议或技术的基于规则的操作。第四，当事人通过自动履行承诺，以一般不可撤销的方式履行承诺。

[0110]智能合同可自动执行不同的流程和操作。在一个实施例中，它们在具有终止性自动执行的基础上自动执行 4iSthis-Then-Then。他们可能会提供 FBR 付款。行动可以以一笔或多笔付款为条件，例如根据付款控制抵押品。

[0111]智能合同可以通过区块链实现。这形成了可在企业对企业实现(B 到 B)和/或对等实现中实现的可信系统。机器对机器的实现允许各种组合。在一个实现中，区块链与构成物联网(LOT)的设备相结合。在另一种组合中，区块链可以与构成物联网的设备与人工智能相结合。通常，该块包含智能合约程序逻辑。它将与特定智能合同相关的消息捆绑在一起，包括输入、输出和逻辑。在又一实施方式中，它们可以提供合约 FBR 差异，例如在使用当前市场价格来调整余额和分散现金流时。

[0112]智能合约是一种信任转移技术。它们降低了交易对手的风险。最好是，这有助于增加信贷。

[0113]智能合同可以在各种模型中实施。它们可能是一份完全用代码写成的合同。它们可以是具有单独自然语言版本的代码中的合同。它们可以是具有编码性能的分裂的自然语言契约。或者，它们可以是具有编码支付机制的自然语言合同。

[0114]智能合同启动需要达成共识。算法构成合同中的每个参与者如何处理消息的一组规则 FBR。它们可以无许可的方式实现，其中任何人都可以提交消息 FBR 处理。提交者可能参与协商一致。或者，他们可以将决策委托给管理员或参与者子组。另一种实现方式是建立一个允许的系统，其中参与者受到限制。它们通常是预先选定的。然后，他们必须接受门禁进入，并必须满足某些要求和/或管理员的批准。

[0115]智能合同适用于不同的订立方法。他们可以通过协议达成协议，例如在有共同的合作机会或确定的预期结果的情况下。这些可能包括商业惯例、资产互换和权利转让。下一步，条件设置 FBR 合同的启动。这可能是由当事人自己决定的，也可能是由某些外部事件的发生造成的，例如时间、其他可量化的度量或地点。通常，他们会生成一个代码，该代码是用区块链技术加密和链接的。它可以被认证和验证。在执行和处理时，网络更新所有分类帐以指示当前状态。一旦验证并发布，它们就不能更改，只能附加其他块。

[0116]重申一下，智能合同作为具有独立内置信任机制的网络上的分布式应用程序。程序赋予价值单位结合规则 FBR 转让价值单位的所有权。它们充当自动执行程序，自动满足程序化关系的条款。

[0117]图 3.。20 示出了作为智能合约实现的彩票实施例。实现抽奖的方法 FBR 包括以下步骤。设置接收加密货币的时间范围。第二，在时间范围内接收带有所有者标识的加密货币。窗口在指定的持续时间内打开 FBR，之后窗口关闭。智能合约例如从随机数生成器生成或接收随机事件。随机数生成器应该包括随机性的算法保证和无黑客攻击的保证。合同在所有者标识相关的加密货币中选择新的所有者(赢家)。然后，它将加密货币的新所有权分配给选定的新所有者(获胜者)。

[0118]智能合同可用于实现核心循环或游戏机制。以下核心环路和游戏机制包括可实现的部分列表，包括但不限于 Jacko、Poko、hotSeat、Hi Lo、Rock、Paper 剪刀、In The Zone 和 iLotto 或其他基于阵列或地理的游戏机制或核心环路。游戏机械师或核心循环的任何子单元本身都可以用作游戏机械师或核心循环。

[0119]Jacko 是一种游戏，包括以下步骤：从具有最小和最大数字的第一数字范围中随机选择目标数字；向玩家呈现目标数字的指示；选择玩家的数字 FBr，该数字从第二范围中选择，具有最小和最大值，其中最大值等于或小于第一范围的最小值；从玩家接收是否再次抽签的指示；如果是，则从第二范围随机选择数字，累加玩家的抽签总数，重复该步骤，直到玩家拒绝抽签或者总数超过目标数目，并且在玩家拒绝抽签的情况下，从第二范围中随机选择数字，累加这些数字，将它们与玩家的累积量进行比较，并且分配总数目最接近但不超过目标的获胜者。

[0120]Poko 是一个多玩家游戏，其中多个标记被授予预定值，而其他玩家没有关于其他玩家持有的至少一些标记的信息。

[0121]高 LO 是一种包括以下步骤的游戏：对一系列随机抽取的数字执行第一次抽奖选择，从玩家接收下一个随机抽取的数字将高于还是低于前一个数字的指示，如果正确，则奖励与随机抽取的数字的数量相关的奖金，并且继续进行，直到玩家无法预测高/低结果，或者选择停止。

[0122]在该区域中是一种碰运气游戏，该游戏包括以下步骤：在预定义的数字范围内随机选择玩家的目标数字，该范围具有最小值和最大值；随机选择彩票游戏中使用的一系列数字 FBR，该预定义数字范围的最小值至少等于最低可能总 FBR 的系列的总和。该数字序列和预定义数字范围的最大值，在选择结束时将随机选择的数字序列合计，并基于玩家数量和总数量的接近度，将奖金金额分配给玩家数量不超过总数的玩家。

[0123]石头布剪刀是一种具有三个或更多选项的游戏，这些选项相对于彼此具有指定的选项优先级。

[0124]竞争席位是一种增加风险/回报的游戏，包括在 Smart ContRact 中选择退出的能力。一种在最终级别达到最终级别的多级机会游戏中进行 FBR 游戏的方法，包括以下步骤：在给定级别呈现多个随机选项，其中至少一个选项是正选项，另一个选项是负选项，以及需要进一步决策的第三选项，接收关于选择多个随机选项中的哪一个的选择，以及如果选择了正选项，则将正选项结果与先前正选项结果累加，但是如果选择了负选项，则累加负选项结果，比较累加结果。以及如果累计次数小于预定次数，则重放相同级别，或者如果累计次数等于预定次数，则终止游戏，并且如果选择了第三选项，则接收关于该决定的选择，尊重上述步骤，直到玩家停止，与发生的预定数量的负面事件或最终级别相关。

[0125]iLotto 是基于网格或地理的系统，包括呈现识别对象的网格的显示器 FBR、接收识别对象的玩家选择的输入 FBR、随机选择获胜识别对象的随机生成器 FBR、以及根据规则向玩家奖励积分的计分系统 FBR，所述规则包括：如果玩家选择的识别对象与获胜的识别对象完全匹配，则第一积分值；如果玩家选择的识别对象与获胜的识别对象具有几何关系，则第二积分值；以及如果玩家选择的识别对象与获胜的识别对象具有几何关系，则第二积分值。

[0126]图 3.。23 涉及执行授权参数和可变参数。强制参数在智能合同中设置。强制参数的示例包括支出百分比和支出金额。可变参数受制于强制参数，提供娱乐选项。

[0127]图 3.。24 描绘了用于电子存储加密货币的钱包。这表示诸如在电话或计算机显示器上的图形用户界面(“GUI”)。各种形式的加密货币可以显示在 GUI 上并存储在钱包中。可以奖励积分，例如 FBR 忠诚度、频率和广播时间。可以列出最近或最近的交易，注明日期、目的和金额。可能会显示总帐户值。

[0128]加密货币系统和智能合约可以与其他系统结合实施。一个额外的系统包括常客或球员的俱乐部系统。它们可能与其他形式的“货币轻量级”相结合，包括微交易和微支付。它们可以与智能资产(即知道其所有者是谁的数字资产或实物)结合使用。数字资产是以数字格式(通常是二进制格式)存在的任何东西，并且有权。

使用。示例包括图像(包括静止图片和视频或动态图像)、可听内容(例如声音、音乐或表演)以及数字文档。所有权通过分布式可信网络控制的财产，例如使用合同的区块链。它们还可以与地理位置结合使用，其中各种组件和建筑组件的物理位置(地理位置)可选地是系统的组件。游戏的地理位置可能会受到限制。该系统可以确保符合数据路由的地理位置。

[0129]无花果。25 至 27 **涉**及具有分离的安全功能和公共功能的系统。这为公共功能和公共实体提供了一个具有多个接口的安全平台。分离的安全功能提供信任代理的功能。安全功能包括以下一项或多项。第一，结果决定。这可能包括使用随机数生成器(RNG)或概率引擎。第二，存储用户或玩家帐户信息。第三，存储货币会计或交易。第四，进行监管和合规接口。第五，开发人员界面等界面。第六，可以提供问答测试、合规性测试和审批等监管职能。

[0130]公共职能包括以下部分或全部。首先，公共系统向安全系统发出‘呼叫’。调用可以通过应用编程接口(API)或 D-API 进行。“open”系统调用调用保护系统 FBR 安全数据。其次，设计器界面用于访问工具、API、开发工具包(DK)和软件开发工具包(SDK)。第三，市场界面充当彩票界面以及可选的应用程序或应用程序商店。第四，操作员接口用于与操作员或组织者(例如慈善机构)对接。它最好服务于出版、营销和销售。第五，用户界面允许注册、播放活动和持久历史记录。

[0131]系统部件可能因功能不同而不同。公共接口和功能优选地包括“开放”平台。这允许 FBR 仲裁并与安全实体达成关于由安全实体执行的游戏操作的协议，例如，支付百分比、可以玩的 vGLEP 和地理位置。安全实体执行安全功能，包括游戏结果、财务事项和安全用户数据。终端用户利用包括但不限于网络、移动应用、移动网络、平板电脑、计算机、支持显示的设备(无线)、零售商处的触摸屏设备(例如，台面游戏)的“频道混合”。私人实体可以施加速率限制并施加负责任的游戏控制。

[0132]无花果。28 和 **29** 描述了混合和分层系统。诸如国营彩票的集中式系统可以与诸如区块链实现的分散式系统相结合。可以在系统内强加分层顺序。在使用强制和可变参数的系统中，可以建立强制参数的分层结构，然后各种可变参数可以服从适当的强制参数。在另一应用中，可以在层次中的较高级别施加全局使用率限制。可以实施分级使用费率限制。系统的各种拓扑结构包括主从式、主从式和循环式。

[0133]图 3.。30 涉及游戏或彩票关联的信用卡和信用卡功能。信用卡和信用功能可以链接到彩票或其他游戏。通过使用信用卡，建立了转换率。例如，FBR 每 100 美元的购买，1 美元的彩票游戏。费率可以是可变的，例如基于机构。在组织或赞助彩票或游戏的慈善组织中，每购买 100 美元，该组织将获得 2 美元的 FBR。也可以执行拆分，例如信用卡所有者在彩票或游戏中每购买 100 美元可获得 1 美元的 FBR，组织可获得 1 美元的 FBR。

[0134]在替代实施例中，移动游戏设备可以通过电缆连接到游戏机，或者直接连接到游戏机的端口，或者经由与游戏机通信的网络连接到游戏机。

[0135]用于根据这里描述的实施例对游戏机和服务器进行编程的软件最初可以存储在诸如 CD 或电子存储设备的 ROM 上。这样的 CD 和设备是其上存储有适当的计算机指令的非暂时性计算机可读介质。该程序也可以通过赌场的网络下载到游戏机上。

[0136]应当理解，这里描述的终端、处理器或计算机可以以多种形式中的任何一种实现，例如机架式计算机、台式计算机、膝上型计算机或平板计算机。此外，计算机可以嵌入通常不被认为是计算机但具有适当处理能力的设备中，该设备包括电子游戏机、网络电视、个人数字助理(PDA)、智能电话或任何其他合适的便携式或固定电子设备。

[0137]此外，计算机可以具有一个或多个输入和输出设备。这些设备尤其可以用来呈现用户界面。可用于提供用户界面的输出设备的示例包括打印机或显示屏、输出的 FBR 可视呈现和输出的扬声器或其他声音生成设备 FBR 可听呈现。可用于用户界面的输入设备的示例包括键盘和诸如鼠标、触摸板和数字化平板的定点设备。作为另一示例，计算机可以通过语音识别或以其他可听格式接收输入信息。

[0138]这样的计算机可以通过任何适当形式的一个或多个网络互连，包括作为局域网或广域网，例如企业网或因特网。这样的网络可以基于任何合适的技术，并且可以根据任何合适的协议操作，并且可以包括无线网络、有线网络或光纤网络。如这里所使用的，术语“在线”指的是这样的联网系统，包括使用例如专用线路、电话线、电缆或 ISDN 线路以及无线传输联网的计算机。在线系统包括使用例如局域网(LAN)、广域网(WAN)、因特网以及上述各种组合的远程计算机。合适的用户设备可以连接到网络 FBR 实例、能够通过网络通信的任何计算设备，诸如台式、膝上型或笔记本计算机、移动站或终端、娱乐设备、与显示设备通信的机顶盒、。

例如电话或智能手机、游戏控制台等无线设备。术语“在线游戏”指的是那些利用这样的网络来允许游戏玩家通过远程和本地的联网或在线系统利用和参与游戏活动的系统和方法。例如，“在线游戏”包括通过互联网上的网站提供的游戏活动。

[0139]此外，这里概述的各种方法或过程可以被编码为可在采用各种操作系统或平台中的任何一种的一个或多个处理器上执行的软件。另外，这样的软件可以使用多种合适的编程语言和/或编程或脚本工具中的任何一种来编写，并且还可以被编译为在框架或虚拟机上执行的可执行机器语言代码或中间代码。

[0140]在这方面，实施例可以提供编码有一个或多个程序的有形、非暂时性计算机可读存储介质(或多个计算机可读存储介质)(例如，计算机存储器、一个或多个软盘、光盘(CD)、光盘、数字视频盘(DVD)、磁带、闪存、现场可编程门阵列或其他半导体器件中的电路配置、或其他非暂时性、有形计算机可读存储介质)，当在一个或多个计算机上执行这些程序时。计算机可读介质或介质可以是可运输的，使得存储在其上的一个或多个程序可以加载到一个或多个不同的计算机或其他处理器上，以实现如上所述的各个方面。如这里所使用的，术语“非暂时性计算机可读存储介质”仅包括可被认为是制品或机器的计算机可读介质，并且不包括暂态信号。在此使用的术语“非暂时性计算机可读存储介质”仅包括可被认为是制品或机器的计算机可读介质，并且不包括暂态信号。

[0141]这里一般意义上使用的术语“程序”或“软件”指的是可用于对计算机或其他处理器编程以实现如上所述的各个方面的任何类型的计算机代码或计算机可执行指令集。另外，应当理解，根据本实施例的一个方面，当执行执行方法的一个或多个计算机程序不需要驻留在单个计算机或处理器上，而是可以以模块化方式分布在多个不同的计算机或处理器之间，以实现在此描述的实施例的各个方面。

[0142]计算机可执行指令可以是由一个或多个计算机或其他设备执行的多种形式，诸如程序模块。通常，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等。通常，在各种实施例中，可以根据需要组合或分布程序模块的功能。

[0143]此外，数据结构可以以任何合适的形式存储在计算机可读介质中。为简单起见，可以将数据结构示为具有通过数据结构中的位置相关的字段。这样的关系同样可以通过为具有计算机可读介质中的位置的字段分配存储来实现，该计算机可读介质传达字段之间的关系。但是，任何。可以使用合适的机制来建立数据结构的字段中的信息之间的关系，包括通过使用指针、标签、地址或在数据元素之间建立关系的其他机制。

[0144]这里描述的实施例的各个方面可以单独使用、组合使用，或者以前述描述的实施例中未具体讨论的各种布置使用，因此这里描述的概念在它们的应用上不限于前述描述或附图中所示的组件的细节和布置。例如，一个实施例中描述的方面可以以任何方式与其他实施例中描述的方面组合。

[0145]此外，这里描述的实施例可以提供一种方法，已经提供了该方法的示例。作为该方法的一部分执行的动作可以以任何合适的方式排序。因此，可以构造以与所示不同的顺序执行动作的实施例，这可以包括同时执行一些动作，即使在说明性实施例中被示为顺序动作。

[0146]虽然已经参考其某些示例性特征描述了实施例，但是本领域技术人员可以对所描述的实施例进行各种修改。这里使用的术语和描述仅用于说明，并不意味着限制。具体地说，尽管已经以示例的方式描述了实施例，但是各种设备将实践在此描述的创造性概念。已经以各种术语描述和公开了实施例，实施例的范围不打算也不应该被认为受其限制，特别是当它们落入这里所附权利要求的广度和范围时，可以由这里的教导建议的其他修改或实施例被特别保留。本领域技术人员将认识到，如以下权利要求及其等价物中定义的那样，这些和其他变体是可能的。尽管出于清楚和理解的目的，通过图示和示例的方式较详细地描述了前述发明，但是根据本发明的教导，本领域的普通技术人员可以很容易地看出，在不背离所附权利要求的精神或范围的情况下，可以对其进行某些改变和修改。

[0147]本说明书中引用的所有出版物和专利在此以引用方式并入，就好像每个单独的出版物或专利被具体地和单独地指示通过引用将其整体并入一样。

参考文献。

[0148]IBM ARM，《2017 物联网商业指数，动态转型》，《经济学人》，智库有限公司 2017，第 1-22 页。

[0149]Crosby 等人的《区块链技术：《超越比特币》，《应用创新评论》，第 2 期，Sutardja Center for EntretreURship&Technology，BerkeLey Engineering，2016 年 6 月，第 1-1.9 页。

[0150]Fisher，《分散式点对点游戏资产平台，使用智能合同与第三方游戏集成》，2014 年 8 月 4 日，12 页。

[0151]Hinton 等，4《深度信念网络的AFast 学习算法》，神经计算，18,1527-1554,2006。

[0152]Jouppi 等人的《张量处理单元 TM 的数据中心内性能分析》，将于 2017 年 6 月 26 日在加拿大多伦多举行的第 44 届国际计算机体系结构研讨会(ISCA)上发表，第 1-17 页。

[0153]LeCun 等人，《深度学习》，《自然》，第 521 卷，2015 年 5 月 28 日，第 436-444 页。

[0154]Marvin，4<区块链 A-Z：关于比特币下的改变游戏规则的技术，你需要知道的一切“，2016 年 6 月 3 日，9 页。

[0155]Marvin，《区块链：《正在改变世界的无形技术》，2017 年 2 月 6 日，32 页。

[0156]Mougayar，The Business BlockChain，第 6-9 页，128-133 页，由 John WiLey&Sons 出版，新泽西州霍博肯。

[0157]Nakamoto，《比特币--点对点电子现金系统》，2008 页。1-9 Ng，《人工智能现在能做什么，不能做什么》，《哈佛商业评论》，2016 年 11 月 9 日，5 页。

[0158]O‘Dowd 等人，《IBM’s Open Blockchain，Making BlockChain Real for Enterprise》，IBM BlockChain，2016 年 4 月，第 1-20 页。

[0159]罗南，《深度学习预测洛托数字》，巴黎学院，2016 年 4 月 1日，第 1-4 页。

[0160]智能合同联盟，“‘智能合同：12 个使用案例 FBR Business and Beyond，A Technology，Legal&Regulatory Information，由智能合同联盟一与德勤(数字商务商会的一个行业倡议)合作编写。2016 年 12 月，第 1-53 页。

[0161]图灵，《计算机器与智能》，思想 49：1950 年，第 433-460 页。

[0162]伍德，《以太：安全分散的通用交易分类账“，宅基地草案，2014 年，第 1-32 页。

[0163]Wu 等人的《Google 的神经机器翻译系统：弥合人与机器翻译之间的鸿沟“，2016 年 10 月 8 日，第 1-23 页。

[0164]Yli-HUUmo 等人，“区块链技术的当前研究在哪里？系统回顾“，2016 年 10 月 3 日，第 1-27 页。

术语表。

[0165]51%攻击：对比特币网络的攻击，允许攻击者创建欺诈性交易，参见 Double Spend。这是可能的，因为控制了比特币网络 50%以上的散列率意味着攻击者可以在计算上胜过所有其他正在挖掘的人。

一个。

[0166]账户：帐户具有作为以太状态的一部分维护的固有余额和交易计数。它们还具有一些(可能为空)EVM 代码和与其关联的(可能为空)存储状态。虽然是同质的，但区分两种实际类型的帐户是有意义的：具有空的关联 EVM 代码的帐户(因此，帐户余额由某个外部实体控制，如果有的话)和具有非空的关联 EVM 代码的帐户(因此，帐户代表自治对象)。每个帐户都有一个单独的地址来标识它。

[0167]地址：比特币地址用于接收和发送比特币网络上的交易。它包含一个字母数字字符串，但也可以表示为。可扫描二维码。比特币地址也是比特币持有者用来对交易进行数字签名的一对密钥中的公钥(参见公钥)。

[0168]地址：用于标识帐户的代码，例如 160 位代码。

[0169]协议分类帐：协议分类帐是两个或多个当事人用来谈判和达成协议的分布式分类帐。

[0170]空投：一种在人群中分发加密货币的方法，2014 年初首次尝试使用 AURoRaco in(AURoRaco In)。

[0171]算法：在计算或其它解决问题的操作中要遵循的过程或规则，尤指计算机所遵循的过程或规则。

[0172]备用币：作为比特币替代品提供的 FBR 加密货币的统称。莱特币、羽毛币和 PPCoin 都是替代币。

[0173]反洗钱:反洗钱技术被用来阻止人们转换非法获得的资金，使其看起来像是合法赚取的。反洗钱机制本质上可以是法律的或技术的。监管机构经常将 AML 技术应用于比特币交易所。

[0174]App：终端用户可见的应用程序，例如托管在以太浏览器中。

[0175]应用程序接口(API)：组件(通常是软件组件)用作彼此通信的接口的规范。可以包括规范 FBR 例程、数据结构、对象类和变量。

[0176]套利：通过在同一资产价格不同的市场之间进行交易而产生的无风险利润。

[0177]ASIC：专用集成电路是专门为完成单一任务而设计的硅芯片。就比特币而言，它们旨在处理 SHA-256 散列问题，以挖掘新比特币。

[0178]ASIC Miner：一种包含 ASIC 芯片的设备，用于挖掘 FBR 比特币。它们可以是插入背板的电路板、带有 USB 连接器的设备，也可以是包含所有必要软件的独立设备，这些设备通过无线链路或以太网电缆连接到网络。

[0179]ASIC 挖掘：许多矿工购买单独的计算设备，完全搁置了 FBR 挖掘。作为另一种选择，他们也可以得到专用集成电路；这是一种专门设计的计算机芯片，用于执行一种特定的功能，在这种情况下，只有一功能，即挖掘计算。ASIC 降低了 FBR 开采所需的处理能力和能源，并可以通过这种方式帮助降低整个过程的成本。无论专用集成电路一(专用芯片本身的术语)是集成到现有的计算系统中，还是作为独立设备运行，术语“专用集成电路”通常指的是整个系统本身，而不仅仅是芯片。

[0180]非对称密钥算法：这是用于生成公钥和私钥的算法，公钥和私钥是加密货币交易必不可少的唯一代码。在对称密钥算法中，发送方和接收方都拥有相同的密钥；它们可以私密地加密和交换信息，但是由于双方都拥有解码信息，所以它们不能对彼此保密。使用非对称密钥算法，双方都可以访问。

公钥，但只有拥有私钥的人才能解密加密；这确保了只有他们才能收到资金。

[0181]认证台账：一种分布式分类帐，提供协议、承诺或声明的持久记录，提供这些协议、承诺或声明已作出的证据(证明)。

[0182]自治代理：在没有人工干预的情况下做出决策并对其采取行动的软件。

[0183]自治对象：仅存在于假设的以太状态中的虚构物体。有一个内部地址，因此有一个关联的帐户；该帐户将具有非空的关联 EVM 代码。仅作为该帐户的存储状态合并。

B 类。

[0184]基数 58：Base58 将二进制数据编码为文本，并用于编码比特币地址。由中本聪(Satoshi Nakamoto)创作，字母数字字符不包括“0”、“O”、“1”、“I”，因为它们很难区分。

[0185]Base58 检查：Base58 的变体，用于检测比特币地址中的键入错误。

[0186]BIP：“比特币改进建议”的首字母缩写，任何想要改善比特币网络的人都可以提交。

[0187]位：比特币面值的名称，等于 100 Satoshis(1 比特币的**百**万分之一)。2014 年，包括比特币(Bitpay)和 Coinbase 在内的几家公司以及各种钱包应用程序都采用了 BIT 来显示比特币金额。

[0188]比特币(大写)：众所周知的加密货币，基于 ProoSof-Work 区块链。

[0189]比特币(小写)：比特币账本使用的具体技术集合，一种特殊的解决方案。请注意，货币本身就是这些技术之一，因为它为矿工提供了开采的动力。

[0190]比特币(货币单位)：一亿，000,000 个智士。一种分散的数字货币单位，可以用来交易商品和服务。比特币也是替代货币生态系统中的一种储备货币。

[0191]比特币 2.0：比比特币白皮书提出的基本支付系统应用更高级或更复杂的比特币或区块链技术的 FBR 应用。比特币 2.0 项目的例子包括对手方、以太、Blockstream、Sarm、Domus 和 Hedgy。

[0192]比特币自动取款机：比特币自动取款机是一种实体机器，允许客户用现金购买比特币。有很多制造商，其中一些可以让用户出售比特币 FBR 现金。它们有时也被称为“BTM”或“比特币 AVMS”。CoinDesk 维护着一张运营比特币 ATM 机的全球地图和一份制造商名单。

[0193]比特币核心：自 2014 年 3 月 19 日发布 0.9 版以来，比特币 Qt 的新名称。不要与 2013 年 8 月发布的 Objective-C 实现 Core 比特币混淆。

[0194]Bitcoind：使用命令行界面的比特币的原始实现。目前是 BitcoinQt 项目的一部分。根据 UNIX 传统，“D”代表 FBR“守护进程”，用于命名后台运行的进程。

[0195]比特币销毁天数：一个估计 FBR 的“货币的速度，与比特币网络。之所以使用这种方法，是因为它赋予了尚未使用的比特币更大的权重。FBR 花费了很长时间，比起每天的总交易量，它更好地代表了使用比特币进行的经济活动的水平。

[0196]比特币投资信托基金：这一私人的开放式信托专门投资于比特币，并代表其股东使用最先进的协议来安全地存储比特币。它为 FBR 的人们提供了一种投资比特币的方式，而不必自己购买和安全地存储这种数字货币。

[0197]比特币 J：迈克·赫恩的完整比特币节点的 Java 实现。除其他功能外，还包括 SPV 实现。

[0198]BitcoinJS：一个在线的 javascript 代码库使用了 FBR 比特币开发，特别是网络钱包、比特币游戏。O 昭(http：//BitcoinJS.org)。

[0199]比特币市场潜力指数(BMPI)：比特币市场潜力指数(BMPI)使用一个数据集对 177 个国家的比特币潜在效用进行排名。它试图展示哪些市场最有潜力采用 FBR 比特币。

[0200]比特币网络：维护区块链的分散的点对点网络。这是处理所有比特币交易的工具。

[0201]比特币价格指数(BPI)：CoinDesk 比特币价格指数代表了符合 BPI 指定标准的全球领先交易所的比特币价格平均值。还有一个 API FBR 开发者可以使用。

[0202]比特币协议：一种开放源码的密码协议，在比特币网络上运行，设定网络如何运行的“规则”。

[0203]BitcoinQt：比特币 Qt 是您的计算机使用的开源软件客户端。它包含区块链的副本，一旦安装，它就会把你的电脑变成比特币网络中的一个节点。还充当“桌面钱包”。**[0204]比特币**-红宝石：朱利安·朗沙德尔(Julian Langschaedel)在鲁比的比特币公用事业图书馆。在 Coinbase.com[0205]比特币情绪指数(BSI)上用于生产：比特币情绪指数是一项衡量个人在任何一天感觉这种数字货币的前景是上升还是下降的指标，该指数是由 Qrious 收集的数据提供支持的。**[0206]比特**币白皮书：这份比特币白皮书是由中本聪(Satoshi Nakamoto)撰写的，并于 2008 年发布在加密技术的邮件列表上。本文详细介绍了比特币协议，中本聪紧随其后，于 2009 年发布了比特币代码。

[0207]比特币白皮书：2008 年 11 月，一篇由中本聪(Satoshi Nakamoto)撰写(很可能是化名)的论文发布在新创建的 Bitcoin.org 网站上，标题为“比特币：一个点对点的电子现金系统。这份长达 8 页的文件描述了使用点对点网络生成“不依赖信任的 FBR 电子交易系统”的方法，并阐述了这种加密货币的工作原理。

[0208]位核：Bitpay 用 JavaScript 编写的比特币工具包。比比特人更完整。

[0209]BitPay：一个支付处理器 FBR 比特币，它与商家合作，使他们能够接受比特币作为支付。

[0210]BitStamp：一种越来越受欢迎的 FBR 比特币交易所。

[0211]区块：这是交易数据的集合，是加密货币的基本要素之一。在进行事务时，收集每个事务的相关信息 FBR，并且当收集的数据达到预定时。

矿藏大小，它被捆绑成一块。区块创建后，尽快由投资者进行 FBR 交易验证；这一过程称为挖掘。

[0212]区块链：自比特币加密货币开始以来已挖掘的块的完整列表。区块链的设计使得每个区块都包含在其之前的区块上的哈希图。这是为了使它更好地防篡改而设计的。更让人困惑的是，还有一家名为 BlockChain 的公司，该公司拥有非常受欢迎的区块链浏览器和比特币钱包。

[0213]区块减半：[参见减半]矿工在开采一个区块时获得的比特币奖励减半。这大约每 4 年发生一次(准确地说是每 210,000 个区块)。

[0214]块头：包含有关块的信息，如前一个块标头的散列、其版本号、当前目标、时间戳和随机数。

[0215]区块高度：区块高度是指区块链中连接在一起的区块数量。例如，高度 0 将是第一个块，也称为创世纪块。

[0216]Blockchain.infb：一种运行比特币节点并显示所有交易和块的统计数据和原始数据的 Web 服务。它还为轻量级客户端 FBR Android、iOS 和 OS X 提供网络钱包功能。

[0217]整体奖励：对成功散列事务块的矿工的奖励。这可能是硬币和交易费的混合，这取决于相关加密货币使用的策略，以及是否所有硬币都已成功开采。比特币目前每个区块奖励 25 个比特币 FBR。当一定数量的区块被开采时，区块奖励减半。以比特币为例，门槛是每 21 万个区块。

[0218]引导：FBR 技术通过几条简单的指令将程序上传到志愿者的计算机或移动设备上，从而启动程序的其余部分。

[0219]BOT 交易：在交易平台上运行的软件程序，通过预先编程的交易指令执行买入和卖出指令。

[0220]大脑钱包：[见钱包]一种比特币钱包，它使用一长串单词来保护其硬币。这个“口令”是可以记住的，让钱包所有者只需记住口令就可以花掉比特币。

[0221]BRainwallet.org：基于比特币的实用程序，可以手工进行交易，将私钥转换为地址，并使用大脑钱包。

[0222]BTC：短货币缩写 FBR 比特币。**[0223]购买订**单：当投资者接近交易所并想要购买加密货币时，就会建立买入订单。这些订单可以是非常简单的订单(“我想在比特币上花费 x 美元”)，也可以是复杂的订单，包括订单应该完成的时间范围、价格范围等因素。大多数交易所允许 FBR 在线输入这些信息，但一些投资者更喜欢直接与交易所代表讨论细节。买入订单并不一定能保证你的购买；如果你的价格太低，比如 FBR，除非你做调整，否则优惠可能会过期而没有得到满足。

C。

[0224]资本管制：这些都是地方性措施，如交易税、限制或其他禁令，政府可以用来监管资本市场流入和流出该国的资金。

[0225]卡萨西乌斯硬币：由迈克·考德威尔生产的实物收藏币。每枚硬币在防篡改的全息图下都包含一个私钥。“Casascius”这个名字是由一个短语“直言不讳”组成的，这是对比特币本身名字的回应。

[0226]总账：中央分类帐是指由中央机构管理的分类帐。

[0227]更改：非正式名称 FBR 交易输出的一部分，在花费该输出后作为“更改”返回给发送方。由于交易输出不能部分花费，所以人们只能将 3 个 BTC 输出中的 1 个 BTC 用于创建两个新输出：一个“付款”输出，其中 1 个 BTC 发送到收款人地址；以及一个“更改”输出，其中剩余 2 个 BTC(减去交易费)发送到付款人地址。BitcoinQt 总是使用密钥池中的新地址，以获得更好的私密性。Blockchain.infb 会发送到钱包中的默认地址。在使用纸质钱包或大脑钱包时，一个常见的错误是将交易更改到不同的地址，然后不小心将其删除。例如，当在临时比特币 QT 钱包中导入私钥时，进行交易，然后删除该临时钱包。

[0228]检查点：块的散列，在此之前，BitcoinQT 客户端在不验证数字签名 FBR 性能的情况下下载块。检查点通常指的是一个非常深的块(至少有几天)，每个人都清楚该块已被绝大多数用户接受，并且重组不会超过该点。它还有助于保护历史上的大部分内容免受 51%的攻击。由于检查点会影响主链的确定方式，因此它们是协议的一部分，必须由替代客户端识别(尽管通过检查点进行重组的风险非常低)。

[0229]圆：Circle 是一项兑换和钱包服务，为全球用户提供存储、发送、接收和交换比特币的机会。

[0230]客户：在台式机、膝上型计算机或移动设备上运行的软件程序。它连接到比特币网络并转发交易。它还可能包括一个比特币钱包(见 Node)。

[0231]云：参考互联网和它可以执行 FBR 任何人的功能，如存储、文件发送和使用应用程序。

[0232]云哈希/挖掘：一种挖掘类型，人们可以付费从云中的其他人那里租用计算机能力，以挖掘比特币或其他加密货币。这是通过出售采矿合同来实现的。CloudHash 也是提供这项服务的企业的名称。

[0233]硬币：一个非正式的术语，意思是 1 个比特币，或者是可以花掉的未花掉的交易产出。

[0234]钱币年代：硬币的年龄，定义为货币数量乘以持有期。

[0235]Coinbase：另一个名字 FBR 是比特币生成交易中使用的输入。当比特币被开采时，它不是来自另一个比特币用户，而是作为对矿工的奖励。这笔奖励被记录为一笔交易，但一些随机数据被用作输入，而不是另一个用户的比特币地址。Coinbase 也是。

比特币钱包服务的名称，该服务还为商家提供支付处理服务，并充当从交易所购买比特币的中介。

[0236]Coinbase.com：总部设在美国的比特币/美元兑换和网络钱包服务。

[0237]冷藏：存储私钥的最安全方式是将它们保存在“冷存储”中，使其离线。这可以是硬件钱包、U 盘或纸质钱包的形式。这些钱包被称为“冷钱包”。

[0238]集体开采：在挖掘数字货币数据块的过程中投入资源和材料往往被证明是太昂贵的 FBR 个人无法参与的。因此，许多有进取心的企业已经想出了一种方法，让那些原本会被排除在外的矿工更容易负担得起采矿费用。这些公司投资于允许 FBR 高端采矿电力的硬件，然后将这种采矿能力的使用权出租给第三方。作为一名个人矿工，这意味着你可以签署一份合同，允许你通过云计算使用预定数量的采矿能力，而不需要购买或维护这样做所需的处理能力的麻烦或费用。成功挖掘数据块所带来的块奖励将归从集体采矿公司购买合同的个人矿工。

[0239]彩色硬币：拟议的 FBR 比特币附加功能，使比特币用户能够赋予他们额外的属性。这些属性可以是用户定义的，使您能够将比特币标记为股票份额或实物资产。这将使比特币能够作为代币、FBR 和其他财产进行交易。

[0240]压缩大小：事务和块序列化中使用的可变长度整数格式的原始名称。也被称为“智史的编码”。它使用 1、3、5 或 9 字节表示任何 64 位无符号整数。小于 253 的值用 1 个字节表示，字节 253、254 和 255 表示后面的 16 位、32 位或 64 位整数。较小的数字可以用不同的方式表示。在比特币-红宝石中，它在比特币 J 中被称为 Varint。BitcoinQt 还具有。更紧凑的表示形式称为 Varint，它与 CompactSize 不兼容，用于块存储。

[0241]确认：将比特币交易成功地散列到交易块中，并巩固其有效性的行为。一次确认大约需要 10 分钟，这是对一个事务块进行散列的平均时间长度。然而，一些更敏感或更大的交易可能需要多次确认，这意味着在交易的区块被散列后，必须对更多的区块进行散列，并将其添加到区块链中。每次在交易的区块之后向区块链添加另一个区块，交易就会再次得到确认。

[0242]确认号：确认号是对交易可能被主链拒绝的概率的度量。“Zero Confirmations‘’表示交易未确认(还没有在任何区块中)。一个确认意味着该交易包含在主链中的最新区块中。两次确认意味着该交易包含在紧挨着最近一笔交易的区块中。事务被反转(“双重花费”)的概率随着“上面”添加更多的块而呈指数级递减。

[0243]已确认交易：已包含在区块链中的交易。交易被拒绝的概率是通过多次确认来衡量的。

[0244]共识要点：一个时间点，或者根据要添加到分类帐中的一组记录数量或数量定义的点，同行在此会面以商定分类帐的状态。

[0245]协商一致进程：该流程由一组负责 FBR 维护分布式分类帐的同行组成，用于就分类帐的内容达成共识。

[0246]合同：非正式术语用于表示可能与帐户或自治对象相关联的一段 EVM 代码。

[0247]核心开发人员：从事开源代码 FBR 比特币的程序员。他们没有正式受雇于比特币网络，也没有被比特币网络支付，也不控制比特币网络；但是，他们在比特币网络的 GitHUb 资源页面 FBR 上拥有更高的访问权，比特币网络的主要“参考”版本就是在这里开发的。

[0248]造假：为了实施欺诈行为而模仿某物的行为。这方面的一个例子是用假币购物。

[0249]CPU：中央处理器--计算机的“大脑”。在早期，这些工具被用来对比特币交易进行散列，但现在已经不够强大了。它们有时仍被用来对 FBR 替代币的交易进行散列。

[0250]众包：为实现一个目标而汇集的资源，如由普通民众贡献的信息或金钱。这通常是通过人们可以捐赠的网站在网上完成的。

[0251]加密货币：一种仅基于数学的货币形式。与印刷的法定货币不同，加密货币是通过基于密码学解决数学问题而产生的。

[0252]加密技术：使用数学来创建可用于隐藏信息的代码和密码。将用于验证和保护比特币交易的数学问题用作基础 FBR。

[0253]CSRNG：首字母缩写 FBR“加密安全随机数生成器”，用于生成私钥 FBR 比特币钱包。

[0254]旋风：由公司通过水力压裂数字世界 FBR 他们的数据创建的。

D。

[0255]DAO：首字母缩写 FBR“分散的自治组织”，一个理论上的公司，可以存在于云中，并根据预设的算法开展业务，不需要人工管理。也称为“DAC”。

[0256]Darksend：Darksend 是黑币的去中心化混合实现，旨在为黑币用户提供更大的交易隐私/匿名性。

[0257]DDoS：分布式拒绝服务攻击使用攻击者控制下的大量计算机来耗尽中心目标的资源。它们通常通过 Internet 发送少量网络流量，以占用目标的计算和带宽资源，从而阻止其向合法用户提供服务。比特币交易所有时会受到 DDoS 攻击。

[0258]深层网络：没有被搜索引擎索引的在线内容使得访问变得困难。互联网上的大部分内容都驻留在深网上，可以使用一种名为 TOR 的程序进行访问。

[0259]滞期费：某些货币惩罚用户囤积 FBR，这是通过滞期费实现的，持有未花掉的硬币要收取 FBR 费用。这项费用会随着时间的推移而增加。

[0260]拒绝服务[DoS]：是对网络的一种攻击形式。比特币节点通过 24 小时禁止其 IP 地址 FBR 来惩罚其他节点的某些行为，以避免 DoS。此外，一些理论上的攻击，如 51%的攻击，可能被用于 FBR 网络范围的 DoS。

[0261]深度：深度指的是区块链中的一个位置。一笔有 6 个确认的交易也可以称为“6 个街区深”。

[0262]桌面钱包：在您的计算机上存储私钥的钱包，它允许您消费和管理比特币。

[0263]确定性钱包：一种基于从称为种子的单个起始点派生多个密钥的系统的钱包。如果钱包丢失，该种子就是恢复钱包所需的全部，并且可以允许在不知道私钥的情况下创建公共地址。

[0264]难度：此数字决定了对新数据块进行散列的难度。它与事务块散列的给定数值部分中允许的最大数量有关。数字越小，生成适合它的散列值就越困难。难度因矿工在比特币网络上使用的计算能力而异。如果 la 昭 e 数量的矿工离开一个网络，难度将会降低。

[0265]数字证书：没有加密-解密操作但用户必须申请(并支付年费)FBR 个人证书的代码片段，大多数常见的电子邮件服务都不支持它们(谷歌、Outlook、雅虎)。

[0266]数码商品：数字商品是一种稀缺的、可电子转让的、无形的、有市场价值的商品。

[0267]数字标识：数字身份是个人、组织或电子设备在网络空间采用或声称的在线或联网身份。

[0268]分布式自治企业[DAE]：几乎不需要或根本不需要传统的管理或层级来创造客户价值和所有者财富。

[0269]分布式应用程序[DAPP]：一套智能合约，将数据存储在房屋列表区块链上。

[0270]分布式资本主义：降低参与门槛。

[0271]分布式台账：分布式分类帐是一种分布在多个站点、国家或机构的数据库。记录一个接一个地存储在连续分类帐中。分布式分类帐数据可以是“允许的”或“不允许的”，以控制谁可以查看它。

[0272]双倍支出：花两次比特币的行为。当某人使用比特币进行交易，然后使用相同的比特币从另一个人那里进行第二次购买时，就会发生这种情况。然后，它们说服网络的其余部分仅通过在块中散列来确认其中一项交易。由于比特币网络的运营方式，双重支出并不容易做到，但对于那些接受零确认交易的人来说，这仍然是一个风险。

[0273]粉尘：交易产出小于花费它所需的典型费用[原文如此]。这不是协议的严格部分，因为任何大于零的值都是有效的。BitcoinQt 拒绝挖掘或中继“灰尘”事务，以避免无用地增加未用事务输出(UTXO)索引的大小。

[0274]粉尘交易：一笔交易的比特币数量极少，几乎没有经济价值，但在区块链中占据了空间。比特币开发团队已经努力通过提高网络转播的最低交易额来消除灰尘交易。

E。

[0275]ECDSA：椭圆曲线数字签名算法是用于对比特币协议中的交易进行签名的轻量级加密算法。

[0276]椭圆曲线算法：在二维椭圆曲线上的一组点上定义的一组数学运算。比特币协议使用预定义曲线 secp256kl。以下是对这些操作最简单的解释：您可以将点加减，然后再乘以一个整数。除以整数在计算上是不可行的(否则加密签名将不起作用)。私钥是 256 位整数，公钥是预定义的点 G(“生成器”)与该整数的乘积：A=G*a。结合性定律允许实现有趣的密码方案，如 Diffie-Hellman 密钥交换(ECDH)：具有私钥 A 和 B 的双方可以交换他们的公钥 A 和 B 以计算共享秘密点 C：C+A*b=B*a，因为(G*a)*==(G*b)*a。该点 C 可以用作 AES 加密密钥来保护它们的通信信道。

[0277]4 娱$^{\text{乐}}$**：**状态、显示、用户体验、刺激(光、声、触觉)、标题/价值转移、游戏[0278]托管：在异步交易期间将资金或资产存放在第三方账户中以保护它们的行为。

[0279]ETF：“交易所买卖基金”的缩写。这些是在股票市场交易的投资基金，跟踪标的资产的价格指数。

[0280]以太浏览器：(也称为 EtherUm Reference Client)类似于简化浏览器(A La Chrome)的界面的跨平台 GUI，它能够托管后端完全基于 EtherUm 协议的沙盒应用程序。

[0281]以太运行时环境：(也称为 ERE)提供给在 EVM 中执行的自治对象的环境。包括 EVM，还包括 EVM 所依赖的世界状态的结构 FBR 某些 I/O 指令，包括 CALL&CREATE。

[0282]以太虚拟机：(也称为 EVM)构成执行模型 FBR 帐户的关联 EVM 代码的关键部分的虚拟机。

[0283]EVM 组件：EVM 代码的人类可读形式。

[0284]EVM 代码：EVM 可以本机执行的字节码。用于向帐户正式指定消息的含义和后果。

[0285]交换：交换不同形式的货币和其他资产的中心资源 FBR。比特币交易所通常用于交换加密货币 FBR 和其他通常为法定货币的货币。

[0286]外部执行者：能够连接到以太节点，但在以太世界之外的人或其他实体。它可以通过存放签署的交易，检查区块链和关联状态，与以太互动。具有一个(或多个)内部帐户。

[0287]额外的随机数：放置在 Coinbase 脚本中的数字，每次 32 位随机数时由挖掘器递增。

整数溢出。当随机数溢出时，这不是继续挖掘所必需的方式，还可以改变事务的 Merkle 树或改变 FBR 使用的公钥，以获得块奖励。

F。

[0288]水龙头：第一次发射替代币时使用的一种技术。预先开采一定数量的硬币，并免费赠送 FBR，以鼓励人们对这种硬币感兴趣，并开始自己开采。

[0289]法定货币：一种凭空创造出来的货币，它之所以有价值，是因为人们说它有价值。由于已知它在洗钱和恐怖活动中的应用，它一直受到监管机构的密切关注。不要与比特币混淆。

[0290]填充或封堵：这是一种使用加密货币交易所发出的简单类型的购买订单。投资者决定他们想要多少货币，以什么价格，并确定订单的截止日期 FBR。然后，交易所将根据这些标准尽最大努力完成订单。如果交易所在截止日期前没有找到合适的匹配 FBR 订单，则订单将被取消且未完成。换句话说，根据这些指导原则并在此时间范围内填写此订单。如果你做不到，就杀了它。

[0291]FinCEN：美国财政部下属的金融犯罪执法网络。到目前为止，FIN-CEN 是对交易所比特币交易实施监管的主要组织。

[0292]叉子：区块链的替代持续版本的创建，通常是因为一组挖掘器开始对一组与另一组不同的事务块进行散列。这可能是恶意造成的，可能是一群矿工获得了对网络的过多控制(参见 51%的攻击)，可能是由于系统中的一个漏洞，也可能是由于核心开发团队决定在新版本的客户端中引入大量新功能时故意造成的。根据难度的定义，如果分支成为区块链的最长版本，那么它就是成功的。

[0293]FPGA：现场可编程门阵列(场 ProgRamming Gate ArRay)是一种处理芯片，可以在制造后配置自定义功能。可以把它想象成一块可以写指令的空白硅板。由于 FPGA 可以批量生产并在制造后配置，制造商从规模经济中受益，使其比 ASIC 芯片更便宜。

[0294]FreiCoin：一种基于经济学家西尔维奥 • 格塞尔(Silvio Gessell)概述的无通胀原则的加密货币。

[0295]无摩擦：就支付系统而言，当交易成本为零或交易限制为零时，系统就是“无功能的”(FHctionless)。

[0296]已满节点：它实现了所有比特币协议，不需要信任任何外部服务来验证交易。它能够下载和验证整个区块链。所有完整节点都实现相同的点对点消息传递协议来交换事务和块，但这不是必需的。完整节点可以使用任何协议并从任何源接收和验证数据。但是，最高的安全性是通过能够尽可能快地与尽可能多的节点通信来实现的。

G。

[0297]燃气：基本网络成本单位。仅由 Ether 支付 FBR 费用(从 PoC-4 开始)，可根据需要自由转换为 Gas。天然气不存在于内部以太计算引擎之外；其价格由交易设定，矿商可以自由忽略天然气价格过低的交易。

[0298]Genesis 区块链中的第一个区块。

[0299]千兆哈希数/秒：给定秒内可能的哈希尝试次数，以数十亿哈希(数千兆哈希)为单位。

[0300]GPU：图形处理单元。硅芯片专门设计了 FBR，这是在现代计算机游戏图形中渲染数百万个多边形所需的复杂数学计算。它们还非常适合于加密货币挖掘所需的加密计算。

[0301]图表间隙：有时，市场价值图上的趋势线会出现缺口。这些差距表明，一种商品的价值出现了明显的下跌或上涨，但这并不一定是因为交易而发生的。这可能是闭市、分析师的统计调整或有关大宗商品的强劲消息的结果。有三种类型的间隙：**[0302]1.**。突破鸿沟(Breakaway Gap)。这些都出现在强劲上涨或下跌趋势的开始，代表着非常大的交易量。

[0303]2.。失控的盖普。这些都发生在上升或下降的趋势中，代表着这一趋势的快速瞬间加剧。

[0304]3.。耗尽差距。这发生在上升趋势或下降趋势接近尾声的时候，并倾向于表明相反方向的小趋势。

H。

[0305]减半：比特币的供应量有限，这使得它们成为一种稀缺的数字商品。比特币的总发行量为 2100 万枚。每个区块产生的比特币数量每四年减少 50%。最后的减半将发生在公元 2140 年。

[0306]硬叉：一些人使用硬叉一词来强调，改变比特币协议需要绝大多数人同意，否则经济中一些引人注目的部分将继续沿用原有的区块链，遵循旧规则。

[0307]硬件钱包：一种比特币钱包，用于在硬件设备上离线存储用户的比特币。

[0308]哈希：一种采用可变数据量并产生较短的固定长度输出的数学过程。散列函数有两个重要特征。首先，通过查看输出很难计算出原始输入是什么。其次，即使更改输入的最小部分，也会产生完全不同的输出。

[0309]要进行散列，请执行以下操作：来计算某些数据的散列函数。如果没有明确提到散列函数，它是由上下文定义的函数。例如，“对事务进行散列”意味着计算事务的二进制表示的哈希 256。

[0310]Hashl60：使用 RIPEMD-160 散列的 SHA-256 用于生成地址，因为它的散列比 SHA-256 小(20 字节比 32 字节)，但仍使用 SHA-256。

256 内部 FBR 安全。核心比特币中的 BTCHashl6O()。BitcoinQt 中的 Hashl60()。它在脚本中也可以作为 op_HASH160 使用。

[0311]散列，散列 256：当不谈到任意哈希函数时，哈希指的是两轮 SHA-256。也就是说，您应该计算数据的 SHA-256 散列，然后计算该散列的另一个 SHA-256 散列。它用于块头散列、事务散列、创建事务的 Merkle 树或计算地址的校验和。在核心比特币中称为 BTCHash2560()，在 BitcoinQT 中称为 Hash()。它也可以在脚本中作为 op_HASH256 使用。**[0312]散列**函数：散列函数接受任意输入，例如整数字符串(键)，并输出预先指定长度的值(散列)。比特币使用加密散列函数来保护网络安全。

[0313]哈希率：比特币挖掘者在给定时间段(通常为一秒)内可以执行的哈希数。

[0314]哈希类型(哈希类型)：附加到事务输入中的事务签名的单个字节，描述应如何对事务进行散列以验证该签名。影响输出的类型有三种：All(默认)、Single、None 和一个影响输入的可选修改器 ANYONECANPAY(可以与前三个中的任意一个组合)。ALL 要求对所有输出进行散列(因此，所有输出都是带符号的)。SINGLE 清除除索引与输入相同的输出脚本之外的所有输出脚本。没有清除所有输出，因此允许随意更改它们。ANYONECANPAY 删除除当前输入之外的所有输入(允许任何人独立投稿)。实际的行为比这个概述更微妙，你应该查看实际的源代码 FBR 更多的注释。

[0315]高度：请参见块高度。

[0316]热钱包：一种可以主动连接到互联网的比特币钱包。这些是 FBR“每天”使用的交易，永远不应该持有大量比特币，因为它们的连通性降低了它们的安全性。

[0317]HTML：首字母缩写 FBR“‘HyperText Markup Language(超文本标记语言)”，即编写网页所使用的语言。

[0318]HTTP：“超文本传输协议”的首字母缩写，这是万维网的底层协议 FBR。**[0319]混合**钱包：这是一个加密货币存储和维护系统，是软件钱包(存储在本地计算机上)和 Web 钱包(存储在第三方服务器上)的组合。你的大部分数字货币账户信息都存储在钱包主机的服务器上--除了 FBR 的一个重要细节。您的私钥(唯一标识您的代码)仅存储在您自己的设备上。当您进行交易时，您的私钥在前往 Exchange 服务器的途中被加密，因此他们永远不会知道您的私钥是什么。访问您的私钥还包括密码，同样只有用户知道。如果用户丢失或忘记该密码，对该帐户的访问可能会被拒绝，并且用户可能会永远失去帐户余额。

我。

[0320]工业区块链：保护手表和其他可穿戴设备的交易功能。

[0321]输入：比特币交易中表示比特币支付来源的部分。通常情况下，这将是一个比特币地址，除非交易是世代交易，这意味着比特币是新开采的(参见 Coinbase)。

[0322]两台或更多台计算机使用它们都能理解的公共语言在诸如因特网的网络上相互交谈的接口系统和方法。

K。

[0323]密钥：可以指 ECDSA 公钥或私钥，或 AES 对称加密密钥。协议本身不使用 AES(仅用于加密 ECDSA 密钥和其他敏感数据)，因此通常单词 Key 表示 ECDSA 密钥。当谈到密钥时，人们通常指的是私钥，因为公钥总是可以从私钥派生出来的。请参见私钥和公钥。

[0324]密钥池：一些创建新私钥的钱包应用程序随机保留一个未使用的预生成密钥池(默认情况下，BitcoinQT 保留 100 个密钥)。当需要新的密钥时，FBR 更改地址或新的支付请求，应用程序提供池中最旧的密钥，并用新的密钥替换它。该池的目的是确保最近使用的密钥始终备份在外部存储上。如果没有密钥池，您可以创建一个新密钥，收到其地址的付款，然后在备份此密钥之前关闭硬盘。密钥池保证该密钥在使用前几天已经备份。确定性钱包不使用密钥池，因为它们需要备份单个密钥。

[0325]KiLohash/秒：给定秒内可能的散列尝试次数，以数千个散列为单位。**[0326]木本**重力井：一种挖掘困难的重新调整算法，创建于 2013 年的 FBR Megaco in，一种替代币。这口井允许在每个区块进行困难的重新调整，而不是每个 2016 个区块 FBR 比特币。这样做是为了回应人们对多池采矿计划的担忧。

[0327]KYC：了解你的客户/客户规则迫使金融机构审查与他们做生意的人，确保他们是合法的。

我。

[0328]洗衣房：比特币也被称为“混合服务”，它们将来自不同用户的资金组合在一起并重新分配，通过混合它们的“污点”，使得追踪比特币的原始来源变得非常困难。

[0329]分类帐：一种仅附加的记录存储，其中的记录是不可变的，并且可能包含比财务记录更多的一般信息。

[0330]所有事项分类帐：区块链可以解决物联网功能正常运行的六个障碍：弹性、健壮、实时、响应、完全开放、可再生、可编辑、创收和可靠。

[0331]杠杆作用：在外汇交易中，杠杆将账户中的实际资金乘以给定的系数，使你能够进行能够带来丰厚利润的交易。通过给予交易员杠杆，交易交易所实际上是借钱给他们，希望它能赚回比借出的佣金更多的钱。杠杆也被称为要求中的最高要求(ma 昭 in Requisition)。

[0332]轻量级客户端：与全节点相比，轻量级节点不存储整个区块链，因此不能完全验证任何事务。轻量级节点有两种：一种是完全信任外部服务来确定钱包余额和交易有效性的节点(如 block chain.infb)；另一种是实现简化支付的应用程序。

产品验证(SPV)。SPV 客户端不需要信任任何特定服务，但比完整节点更容易受到 51%的攻击。请参阅：简化付款验证。

[0333]Litecoin：一种基于解密工作证明的替代币。

[0334]流动性：轻松买卖资产的能力，交易之间的定价大致相同。适度庞大的买家和卖家群体对于流动性非常重要。缺乏流动性的市场的结果是价格波动，无法轻松确定资产的价值。

[0335]流动性互换：作为加密货币交易所的一种金融工具，流动性掉期是投资者向他人提供贷款进行交易的合约，以换取 FBR 的固定回报。

[0336]LLL：类 Lisp 的低级语言，一种人类可写的语言，使用 FBR 编写简单的合同和通用低级语言工具包 FBR 反编译为。

[0337]锁定时间(锁定时间)：事务中的 32 位字段，表示事务生效的块高度或 UNIX 时间戳。零表示事务在任何块中都有效。小于 500000000 的数字被解释为块号(11000 年后将达到限制)，否则为时间戳。

[0338]彩票：被许多州定义为奖赏、机会和代价。

M。

[0339]MAC 媒体访问控制。

[0340]主链：区块链的一部分，节点认为这是最困难的(参见困难)。所有节点存储包括孤儿在内的所有有效块，并在接收到另一个块时重新计算总难度。如果新到达的一个或多个块没有扩展现有的主链，而是从先前的某个块创建另一个主链，则称为重组。

[0341]主网：主要的比特币网络及其区块链。该术语主要用于与 Testnet 进行比较。

[0342]mBTC：千分之一比特币(0.001 比特币)。

[0343]兆哈希数/秒：给定秒内可能的哈希尝试次数，以百万哈希(数千 KiLohash)为单位。

[0344]Mempool：术语 FBR 是节点存储的未确认事务的集合，直到它们到期或包含在主链中。当重组发生时，孤立块中的事务要么变为无效(如果已经包含在主链中)，要么移到未确认事务池中。默认情况下，bitcoind 节点在 24 小时后丢弃未经确认的事务。

[0345]合并采矿：这允许矿工同时在多个区块链上工作，从而提高了被挖掘的两种货币的散列率(从而提高了安全性)。例如，Namecoin 已经实现了与比特币的合并挖掘。

[0346]Merkle Tree：Merkle 树是一种抽象数据结构，它将数据项的列表组织在散列树中(就像在 Git、MercURial 或 ZFS 中一样)。在比特币中，Merkle 树仅用于组织块内的事务(块标题只包含树的一个散列)，因此满节点可以修剪全部耗尽的事务以节省磁盘空间。如果向 SPV 客户端提供了所有中间散列的列表，则 SPV 客户端仅存储块标头并验证事务。

[0347]消息：通过自治对象的确定性操作或事务的加密安全签名在两个帐户之间传递的数据(作为一组字节)和值(指定为以太)。

[0348]留言电话：将信息从一个账户传递到另一个账户的行为。如果目标帐户与非空的 EVM 代码相关联，则 VM 将以所述对象的状态和所操作的消息启动。如果消息发送者是自治对象，则调用将传递从 VM 操作返回的所有数据。

[0349]小额交易：支付少量 FBR 来购买资产或服务，主要是在线支付。小额交易在传统支付系统下很难进行，因为涉及的佣金很高。以 FBR 为例，用你的信用卡阅读一篇在线文章很难花 2 美分。

[0350]矿工：参与任何加密货币网络执行工作证明的计算机。这通常是为了获得大宗奖励。

[0351]采矿：通过使用计算硬件解决密码问题来生成新比特币的行为。**[0352]挖掘**算法：加密货币用来对比特币网络中的交易进行签名的算法，将区块添加到区块链上。

[0353]采矿合同：一种投资比特币挖掘硬件的方法，允许任何人在约定的时间内出租预先指定数量的散列能力。矿业服务负责硬件维护、托管和电力成本，使其成为更简单的 FBR 投资者。**[0354]矿池**：一群矿工决定将他们的计算能力结合起来进行 FBR 挖掘。这使得奖励可以在池中的参与者之间更一致地分配。

[0355]铸币厂：Satoshi 通过将比特币的发行与创建新的区块分类账联系起来分发铸币，将铸币的权力交到了同行网络的所有人手中。

[0356]铸币帽：当加密货币矿工处理交易数据块时，他们会因此产生新的硬币。加密货币是一个年轻的行业，其发行人希望有足够的硬币流通，以满足新投资者的加入。这些新硬币的数学设计是以稳定的速度生产，因此货币的价值也将保持相对稳定(就像在任何其他大宗商品市场一样，会有波动，但不会像商品供应极其有限的情况下那样疯狂)。然而，随着时间的推移，硬币创造的数学也被设计为结束，以避免市场过饱和和货币贬值。

[0357]铸币：在证明赌注硬币时奖励使用者的过程。新硬币被铸造，作为 FBR 在一块内验证交易的奖励。

[0358]混合：为了增加个人历史的私密性而与他人交换硬币的过程。有时它与洗钱联系在一起，但严格地说，它与洗钱是正交的。在传统银行业务中，银行通过向所有第三方隐藏交易来保护客户隐私。在比特币中，任何商家都可以对一个人的整个支付历史进行统计分析，并确定一个人拥有多少比特币，比如 FBR。虽然仍然可以在每个商家的级别上实施 KYC(了解您的客户)规则，但混合允许在 MER 之间提供关于个人历史的单独信息。

圣歌。最重要的FBR混合使用案例包括：1)拿到一份月薪，然后花在小额交易中(“当你只付4美元时，咖啡馆就会看到数千美元”)；2)一次付款，揭示出许多小额私人支出之间的联系(“汽车经销商看到你有多沉迷于小圈子”)。在这两种情况下，你的雇主、咖啡馆和汽车经销商可能会遵守KYC/AML法律，并报告你的身份和转账金额，但他们都不需要知道对方的情况。在拿到工资后混合比特币，然后在支付大笔款项之前混合比特币，就解决了这个隐私问题。

[0359]混合服务：一种将你的比特币与其他人的比特币混合在一起的服务，将你发送给比特币的比特币与分隔符输入和输出一起发回给你。混合服务(也被称为TUmbler)保护了你的隐私，因为它阻止人们追踪特定的比特币到你。它还有可能被用于FBR洗钱。

[0360]移动钱包：这是一种运行“移动客户端”的钱包，人们可以在手机和平板电脑上使用比特币钱包，并在移动中进行支付。

[0361]货币政策：另一个突破是保留软件中编程的价值。

[0362]洗钱：通过将犯罪活动中赚取的利润转化为看起来合法的资产，试图“清理”这些钱的行为。

[0363]M-of-N多重签名交易：需要N个公钥(M小于或等于N)时可以使用M个签名进行的事务。只包含一个OP_CHECKMULTSIG操作码且N为3、2或1的多重签名事务被视为标准事务。

[0364]多重签名：多重签名地址允许多方使用公钥部分播种地址。当有人想要花掉一些比特币时，除了他们自己之外，他们还需要这些人中的一些人签署他们的交易。当人们创建地址时，所需的签名数量在开始时就已达成一致。使用多重签名地址的服务具有更强的防盗能力。

n。

[0365]Namecoin：一种替代币，旨在提供传统域名系统(DNS)的替代方案。用户可以通过域名支付来注册.bit域，可以通过代理服务器访问。

[0366]网络效应：增值当一种商品或服务的使用变得更加广泛时，它的价值就会增加。**[0367]NFC：**近场通信是“近场通信”的缩写，是一种低功耗、短距离的无线通信方法。这可以用于构建RFID系统，也是非接触式智能卡(牡蛎卡)和支付系统(PayPass)的用途。最近在Apple Pay应用程序中实现了这一功能。

[0368]节点：使用客户端连接到比特币网络的计算机，该客户端将交易中继给其他人(请参阅客户端)。**[0369]随机数：**在对事务块进行散列时用作输入的随机数据字符串。现时值用于尝试生成符合比特币难度设置的数字参数的摘要。每次散列尝试将使用不同的随机数，这意味着在尝试散列每个事务块时会生成数十亿个随机数。

[0370]非标交易：任何非标准的有效交易。非标准交易不包括。默认情况下中继或挖掘BitcoinQt节点(但在Testnet上中继和挖掘)。但是，如果任何人将此类事务放入块中，则所有节点都会接受该事务。在实践中，这意味着不寻常的交易需要更多时间才能纳入区块链。如果某种非标准事务变得有用和流行，它可能会被命名为标准，并被用户(喜欢)采用。请参阅标准事务处理。

[0371]诺瓦科因：尽管这种类型的加密货币还没有接近该行业大型参与者的价值或整体投资者数量，但Novaco in仍在前五名中占有一席之地；考虑到它是在2013年2月推出的，这还不错。Novaco in使用SCRYPT挖掘算法，并结合使用prooSoSwork和prooSof-Start方法进行挖掘。

O。

[0372]对象：同义词FBR自治对象。

[0373]关闭区块链交易：信任方之间发生在区块链之外的价值交换。之所以会出现这些情况，是因为它们速度更快，并且不会阻止区块链。

[0374]账外币种：梅杰铸造的一种货币，在分类账上使用。这方面的一个例子是使用分布式分类账来管理国家货币。

[0375]分类帐上币种：一种铸造在分类账上并在分类账上使用的货币。这方面的一个例子是加密货币。

[0376]操作码：脚本操作的8位代码。从0x01到0x4B(十进制75)的代码被解释为要推送到解释器堆栈上的数据长度(操作码后面是数据字节)。其他代码要么做一些有趣的事情，要么被禁用并导致交易验证失败，或者什么都不做(保留FBR将来使用)。

[0377]开放网络企业：随着智能合约变得越来越复杂，并与其他合约进行互操作，这就促成了这一点。

[0378]开源：共享一款计算机软件的源代码，允许任何人分发和修改它的做法。

[0379]孤岛：该块不是有效区块链的一部分，而是被丢弃的分叉的一部分。

[0380]场外交易所：交易员之间直接进行交易，而不是依靠中央交易所进行调解的交易所。

[0381]产量：目的地址是比特币交易的FBR。单个事务可以有多个输出FBR。

[0382]硬币拥有者：以太选择了这一点作为它的经济设置。涟漪和明星选择了社交网络。

[0383]计算能力的拥有者：智史选择了这个经济模式。这就要求这些矿工要想参与奖励制度，就必须消耗网络之外的一种资源，即电力。

P。

[0384]纸质钱包：包含一个或多个公开比特币地址及其对应私钥的打印页。通常用于安全地存储比特币，而不是使用软件钱包或网络钱包，因为软件钱包可能会被破坏，网络钱包可能会被黑客入侵或干脆消失。一种有用的冷比特币存储形式。

[0385]参与者：可以访问分类帐的参与者：读取记录或将记录添加到。

[0386]Pay-to-Script 哈希：一种脚本和地址类型，允许使用任意复杂脚本的紧凑散列将比特币发送到该脚本。这使得付款人支付的交易费要少得多，而不需要等待很长时间 FBR 非标准交易才能纳入区块链。则在兑换资金时必须由收款人提供与散列匹配的实际脚本。P2SH 地址采用 Base58 校验编码，就像普通公钥一样，并以数字“3”开头。

[0387]同行：共同承担责任的行为者，负责维护分类账的身份和完整性。

[0388]P2P：点对点。高度互联网络中至少两方之间发生的分散交互。一种替代“中心辐射式”安排的系统，在这种安排下，交易中的所有参与者都通过单一的中介点进行交易。

[0389]许可分类帐：授权分类帐是一种分类帐，参与者必须具有访问分类帐的权限。授权分类帐可以有一个或多个所有者。当添加新记录时，通过有限的协商过程检查分类帐的完整性。这是由受信任的参与者一政府部门或银行执行的，例如 fbr-这使得维护共享记录比未经许可的分类账使用的协商一致过程简单得多。被许可的区块链提供了高度可验证的数据集，因为协商一致过程创建了一个数字签名，所有各方都可以看到。许可的分类帐通常比未经许可的分类帐快。

[0390]电话到电话转接：这是一种移动应用程序功能，允许将信息从一部智能手机即时传输到另一部智能手机。如果两个移动设备用户想要交换数据，并且都在他们的电话上安装并激活了此功能，他们只需将他们的设备放在彼此很近的地方就可以进行传输。这些有时也被称为“触摸传输”。

[0391]平台交换：这是一个数字货币交易所，限制了它们在投资者之间进行的交易中发挥的作用。大多数交易所都是为了促进这些交易，并使它们更容易进行。该交易所将对买入和卖出订单进行分类，然后将符合相关订单标准的投资者进行匹配。他们的算法经过精心设计，使得交易对双方都是安全和公平的。不过，除此之外，交易所并不扮演任何“中间人”或调停角色。这与交易所形成鲜明对比，交易所将以第三方托管交易资金，或者在推进交易之前与两家投资者讨论交易细节。

[0392]池：一群采矿客户，他们共同开采一个区块，然后在他们之间平分报酬。随着难度的增加，矿池是增加成功开采区块的概率的有效方法。

[0393]PPCoin：也就是点对点硬币或点对点硬币。一种将赌注证明机制与工作证明相结合的替代币。根据桑尼•金和斯科特•纳达尔撰写的一篇论文。

[0394]开采前：在一种加密货币的创始人开采硬币之前，该硬币还没有被宣布，细节也被公布给了其他可能想要开采硬币的人。预采是一种常用的预采技术，尽管并不是所有预采的硬币都是预采的(见 ScamCoin)。

[0395]Primecoin：由 Sunny King 开发的 Primecoin 使用工作证明系统来计算素数。

[0396]私钥(PrivKey)：由用户保密的字母数字字符串，用于在使用公钥进行散列时对数字通信进行签名。就比特币而言，此字符串是专为使用公钥而设计的私钥。公钥是比特币地址(参见比特币地址)。

[0397]流程节点：在芯片制造过程中产生的以纳米为单位的晶体管尺寸。流程节点越小，效率越高。

[0398]活动证明：把工作证明和赌注证明结合起来。

[0399]爆炸证明：这是一种“烧录”一种工作证明加密货币以获得另一种加密货币的方法。这是一种将一种加密货币从另一种加密货币上“自举”的形式，通过将硬币发送到一个可验证的不可消费地址来实现。

[0400]能力证明：要求矿工将相当数量的硬盘分配给采矿。

[0401]存在证明：一项通过区块链提供的服务，允许任何人匿名和安全地存储存在的证明，FBR 任何他们选择的在线文档。这使人们能够证明文档在某个时间点存在，并证明他们对文档的所有权，而不必担心证据会从他们手中夺走。

[0402]桩的证明：工作证明的另一种选择，即你在一种货币中的现有股份(你持有的该货币的金额)被用来计算你可以开采的该货币的金额。

[0403]存储证明：需要挖掘者在分布式云中分配和共享磁盘空间。

[0404]工作证明：一种将挖掘能力与计算能力捆绑在一起的系统。必须对块进行散列，这本身就是一个简单的计算过程，但是在散列过程中添加了一个额外的变量使其更加困难。当成功地对块进行散列时，散列必须花费一些时间和计算工作量。因此，哈希块被认为是工作的证据。

[0405]消费者：生产产品的客户。

[0406]协议演变：区块链是互联网协议自然演变的结果。《连线》讲述了 1974 年最初的 TCP/IP 互联网网络协议和 Tim Berner-Lee 的超文本传输协议(HTTP)是如何以与区块链相同的方式演变的，正在演变为下一代互联网，将多种协议捆绑在一起形成未来框架的基础，并“从头看着互联网的诞生”。

[0407]PSP：支付服务提供商。PSP 为希望接受在线支付的 FBR 商家提供支付处理服务。

[0408]P2SH：请参见付费脚本哈希。

[0409]公钥(PubKey)：一种公知的字母数字字符串，它与另一个私人持有的字符串进行散列以签署数字通信。在比特币的情况下，公钥是比特币地址。

问。

[0410]二维码：包含表示以下序列的单色图案的二维图形块。

数据。二维码，即“快速响应”码，是为摄像头(包括手机中的摄像头)扫描而设计的，经常被用来对比特币地址进行编码。

R。

[0411]参考实施：比特币 Qt(或位编码)是使用最多的全节点实现，因此它被认为是其他实现的参考。如果替代实现与 bit-coinQt 不兼容，它可能会被分叉，也就是说，它将不会看到与运行 BitcoinQT 的网络的其余部分相同的主链。

[0412]中继交易：相互连接的比特币节点在尽力的基础上相互中继新的交易，以便将它们发送到挖掘节点。有些事务可能不是由所有节点中继的。例如非标准交易，或者没有最低费用的交易。比特币信息协议并不是发送交易的唯一方式。也可以直接寄给矿工，自己挖矿，或者直接寄给收款人，让他们转送或挖矿。

[0413]汇款：汇款通常在国际上作为付款或礼物寄出的一笔钱。

[0414]REO 昭，REOI^ANIZATION：当主链中的一个或多个块变为孤立时节点中的事件。通常，新收到的数据块是对现有主链的扩展。有时(每周 4-6 次)几乎同时产生几个相同高度的块，并且 FBR 在短时间内，一些节点可能会将一个块视为主链的顶端，最终将被更难的块所取代。孤立块中的每个事务要么变为无效(如果已包含在主链块中)，要么变为未经确认并移至内存池。如果出现重大错误或 51%的攻击，重组可能涉及重组多个块。

[0415]复制分类帐：具有一个主(授权)数据副本和多个从(非授权)副本的分类帐。

[0416]奖励：矿工可以在新区块中认领的新生成比特币的数量。该区块的第一笔交易允许矿商要求目前允许的奖励，以及从该区块所有交易的所有交易费中收取交易费。奖励大约每 4 年减半 210000 个街区。截至 2014 年 7 月 27 日，奖励为 25BTC(第一次减半发生在 2012 年 12 月)。出于安全原因，奖励不能在 100 个街区之前花掉，这些街区是在现有图书的基础上建造的。

[0417]波纹：可用于转移任何货币(包括用户创建的临时货币)的支付网络。该网络由当局运营的支付节点和网关组成。支付使用一系列逻辑单元，网络基于信任关系。

%s。

[0418]智史：目前可用的比特币的最小细分(0.00000001 比特币)。

[0419]中本聪：比特币协议的最初发明者使用的名字，他于 2010 年底退出了该项目。

[0420]假币：一种替代币，其唯一目的是让发起人赚钱。Scamcoins 经常使用抽水和倾倒技术，并一起进行预开采。

[0421]脚本：一种紧凑的图灵不完全编程语言，用于事务输入和输出。脚本由类似 Forth 的堆栈机器解释：每个操作都操作堆栈上的数据。大多数脚本遵循标准模式，并对照前一事务输出中提供的公钥验证事务输入中提供的数字签名。签名和公钥都是使用脚本提供的。脚本可能包含复杂的条件，但永远不能更改正在传输的金额。金额存储在事务输出的单独字段中。

[0422]scriptPubKey：Bitcoind FBR 中的原始名称是事务输出脚本。通常，输出脚本包含公钥(或其散列：请参见地址)，这些公钥只允许相应私钥的所有者兑换输出中的比特币。

[0423]scriptSig：Bitcond FBR 事务输入脚本中的原始名称。通常，输入脚本包含签名以证明先前交易发送的比特币的所有权。

[0424]加密：SHA-256 的替代工作证明系统，设计为对 CPU 和 GPU 矿工特别友好，而对 ASIC 矿工几乎没有优势。**[0425]密钥**：加密钱包中使用私钥或加密密钥。比特币协议在任何地方都不使用加密，因此密钥通常意味着使用 FBR 签名交易的私钥。

[0426]顺序：事务输入中的 32 位无符号整数，用于将事务的旧版本替换为新版本。仅在锁定时间不为零时使用。直到序列号为 OxFFFFFFFF，交易才被视为有效。

[0427]种子：确定性钱包中使用的私钥。

[0428]自动执行合同：也称为“智能合同”，这些协议在不需要 FBR 人工干预的情况下促进或执行合同义务。

[0429]国家环保总局：欧洲单一支付区。欧盟内部的一项支付一体化协议，旨在使不同银行和国家之间以欧元进行资金转移变得更容易。

[0430]SHA-256：作为 FBR 比特币工作证明系统基础的加密函数。

[0431]侧链：这些都是理论上独立的区块链，与比特币区块链“双向挂钩”。它们可以有自己的独特功能，并可以将比特币发送到它们和从它们接收比特币。

[0432]签名：通过将私钥和公钥散列在一起来证明比特币交易来自特定地址而生成的数字摘要。

[0433]简化支付验证(SPV)：一种无需存储整个区块链(仅区块标头)和不信任任何外部服务来验证事务的方案。每个事务必须存在于 Merkle 树中直到根的所有父哈希和兄弟哈希中。SPV 客户端信任最困难的块头链，并可以验证事务是否确实属于某个块头。由于 SPV 不会验证所有交易，51%的攻击可能不仅会导致双倍开销(就像 Full 一样。

节点)，而且还使用从任何地方创建的比特币进行完全无效的支付。然而，这种攻击的成本非常高，而且可能比相关产品更贵。BitcoinJ 库在功能上实现了 SPV。(参见 SPV)。

[0434]智能合同：智能合同是以计算机语言而不是法律语言记录条款的合同。智能合约可以由诸如合适的分布式分类帐系统的计算系统自动执行。

[0435]软叉：有时，软分叉指的是软件行为的一个重要变化，而不是硬分叉(例如，改变挖掘费政策)。请参见硬叉和叉子。

[0436]源代码：开放源码软件，包括管理比特币规则、FBR、移动和所有权的协议，以及保护和验证比特币交易的密码系统。

[0437]投机者：投机比特币或任何其他形式资产价格的个人。旨在通过以不同的价格买卖来赚取利润。

[0438]消耗产量：事务输出只能使用一次：当另一个有效事务从其自己的输入引用此输出时。当另一个事务试图花费相同的输出时，它将被已经看到第一个事务的节点拒绝。区块链作为一种 ProoSof-Work 方案，允许每个节点就哪一笔交易确实是第一笔交易达成一致。当整个事务的所有输出都用完时，就认为整个事务已用完。

[0439]泄漏：区块链的分裂。请参见叉子。

[0440]SPV：简化付款验证。比特币协议的一项功能，使节点无需下载完整的区块链即可验证支付。相反，他们只需要下载块头。

[0441]陈旧：当一个比特币块被成功散列后，任何其他试图散列它的人都可能会停止，因为它现在已经“过时”了。他们只是在重复别人已经做过的工作，FBR 没有报酬。这个术语也用在挖掘池中，用来描述已经完成的散列作业的份额。

[0442]陈旧区块：一个已经解决的区块，因此不能为矿工提供任何奖励，FBR 在它上面做进一步的工作。

[0443]标准交易：有些事务被认为是标准事务，这意味着它们由大多数节点进行中继和挖掘。更复杂的事务可能有漏洞或导致网络上的 DoS 攻击，因此它们被认为是非标准的，不会被大多数节点中继或挖掘。标准和非标准交易都是有效的，一旦被纳入区块链，将被所有节点识别。标准事务处理包括：1)发送到公钥，2)发送到地址，3)发送到 P2SH 地址，4)发送到 N 为 3 或更小的 M-OSN 多重签名事务。

[0444]存储状态：在帐户的关联 EVM 代码运行期间维护的特定于给定帐户的信息。

T。

[0445]污点：当两个地址都持有特定比特币时，对这两个地址关联程度的分析。污点分析可以用来确定 FBR 比特币从已知 FBR 被盗硬币的地址移动到当前地址需要多少步骤。

[0446]目标：一个 2.56 位的数字，它将上限 FBR 设置为有效的块头散列。目标越低，找到有效人选的难度就越高。最大(最容易)的目标是。0X00000000FFFF000000000000000000000000000000000000000000000000。难度和目标每隔 2016 个区块调整一次(约。2 周)以保持块之间的间隔接近 10 分钟。

[0447]TCP/IP: 首字母缩写代表 FBR“传输控制协议(TRansfer Control ProtocorV)、互联网协议(Intemet Protocol)”，是互联网使用的连接协议。

[0448]兆兆字节/秒：给定秒内可能的哈希尝试次数，以万亿哈希(千兆哈希)为单位。

[0449]测试网：另一种比特币区块链，纯粹用于 FBR 测试目的。

[0450]测试 3：带有另一个创世模块的最新版本的 Testnet。

[0451]时间戳：证明某一数据在某一时间点存在的证据。对于比特币来说，这是交易何时发生的加密证据。

[0452]无令牌分类帐：无代币分类账是指不需要本币操作的分布式分类账。

[0453]TOR：一种匿名路由协议，供想要在网上隐藏身份的人使用。

[0454]硬币总供应量：对于许多加密货币来说，将会出现的硬币总数是有限制的，比特币的总供应量上限为 2100 万枚。

[0455]交易记录：一条数据，由外部演员签名。它表示消息或新的自治对象。交易记录到区块链的每个区块中。

[0456]交易区块：比特币网络上的交易集合，收集成一个区块，然后可以进行散列并添加到区块链中。

[0457]交易数据库：从纯技术角度来看，区块链是交易数据库。散列、键和节点都构成了一个避开集中式存储的分布式数据库。

[0458]交易费：对通过比特币网络发送的一些交易征收的一小笔费用。交易费奖励给成功散列包含相关交易的块的挖掘器。

[0459]交易录入：事务的一部分，其中包含对前一个事务的输出的引用，以及可以证明该输出所有权的脚本。脚本通常包含签名，因此称为 scriptSig。投入完全消耗了之前的产出。因此，如果只需要支付以前输出的一部分，事务应该包括额外的更改输出，将剩余的部分发送回其所有者(在相同或不同的地址上)。Coinbase 事务只包含一个输入，该输入带有对前一个事务的零引用和替代脚本的任意数据。

[0460]交易产出：输出包含要发送的金额和允许进一步支出的脚本。脚本通常包含公钥(或公钥的地址、散列)和签名验证操作码。只有相应私钥的所有者才能创建另一个事务，该事务将该金额进一步发送给某些-。

另一个。在每笔交易中，产出金额的总和必须等于或小于所有投入金额的总和。请参见更改。

[0461]TX：请参阅交易记录。

[0462]TXIN：请参阅：事务处理输入。

[0463]TXOUT：请参阅交易输出。

使用。

[0464]无处不在：区块链无处不在；在字母表中，这已经不是什么新闻了。开放源码，区块链的普遍适用的架构，以及它们分发、匿名、保护和保持完美准确的网络交易记录的能力，使这项技术成为既定技术。

[0465]Ubtc：一枚微比特币(0.000001 比特币)。

[0466]未确认交易：不包括在任何块中的事务。也称为“O-确认”交易。未确认的事务由节点中继，并留在内存池中。未经确认的事务会一直留在池中，直到节点决定将其丢弃、在区块链中找到它、或将其包含在区块链中、或将其包含在区块链本身中(如果它是挖掘器)。请参阅确认号。

[0467]唯一节点列表：其他区块链，如 Ripple 和 Stella，依赖于社交网络 FBR 共识，并可能推荐新的参与者(即新的节点)来生成唯一的模式列表。

[0468]未经许可的分类帐：比特币等未经许可的账簿没有单一所有者-实际上，它们不能被拥有。未经许可的分类帐的目的是允许任何人向分类帐提供数据，并允许所有拥有分类帐的人拥有相同的副本。这会产生阻力，这意味着没有参与者可以阻止将交易添加到分类帐中。参与者通过就分类账的状态达成共识来维护分类账的完整性。

[0469]UTXO 设置：未使用的事务输出的集合。通常用于讨论如何优化尚未花费的事务输出的不断增长的索引。索引对于有效验证新创建的事务非常重要。即使新事务的速率保持不变，查找和验证未花费的输出所需的时间也会增加。可能的技术解决方案包括更高效的索引算法和更完善的硬件。例如，BitcoinQT 只保存与用户键匹配的输出的索引，并在验证其他事务时扫描整个区块链。一位网络钱包服务的开发者提到，他们维护着 UTXO 的整个索引，当区块链本身只有 GB 的时候，它的大小在 100 GB 左右。一些人寻求社会方法来解决这个问题。例如，通过拒绝中继或挖掘被认为是粉尘的交易(包含的产出小于开采/中继它们所需的交易费)。

V

[0470]虚荣地址：具有所需模式(如名称)的比特币地址。

[0471]瓦林特：这个术语可能会引起混淆，因为它意味着不同比特币实现中的不同格式。请参见压缩大小。

[0472]货币流通速度：货币流通速度是衡量收到的钱再次花掉的速度的一个指标。对于比特币，我们用“比特币销毁天数”来衡量其速度，这可以表明人们是在囤积比特币还是在消费比特币。

[0473]核查：区块链在没有验证的情况下不会作为分类账工作。这在很大程度上取决于矿工，他们的区块创建软件在将交易捆绑成区块时，会验证交易的散列。在加密货币和银行场景中，支付验证也是至关重要的。这一验证通过分布式网络中的节点通信进行，在发送比特币交易之前，将其与每个节点的区块链数据进行交叉检查。

[0474]维珍比特币：购买比特币作为奖励，FBR 挖掘一个区块。这些钱还没有花在任何地方。

[0475]波动性：对一段时间内价格变动的测量 FBR 是一种交易的金融资产(包括比特币)。

W

[0476]钱包：一种存储比特币的方法，供以后使用。钱包持有与比特币地址相关联的私钥。区块链是与这些地址关联的比特币金额的记录。

[0477]钱包：就像纸币和硬币钱包一样，这里是存放数字货币的地方。加密货币钱包有四种类型：

[0478]1.。软件钱包。这些程序是您加载到台式机或笔记本电脑上的程序。

[0479]2.。移动钱包：这些应用程序以您在智能手机或平板电脑上安装的应用程序的形式出现。它们通常包括二维码扫描和电话到电话转账 FBR On-The-Go 交易。

[0480]3.。网络钱包：这些数据通常通过交换获得，并通过云计算存储在第三方服务器上。它们可以被任何计算设备访问。

[0481]4.。纸质钱包：你的数字货币可以打印出来，通常以二维码的形式打印出来，这些硬拷贝的加密货币“钞票”可以像传统货币一样保存在实体钱包里。

[0482]电汇：通过电子方式把钱从一个人转到另一个人。通常用于从比特币交易所发送和检索法定货币。

X。

[0483]XBT：1 比特币的非正式货币代码(定义为 100 000 000 Satoshis)。一些人建议使用 FBR 0.01 比特币，以避免与比特币混淆。有传言称，彭博社将 XBT 测试为 FBR 1 比特币，但目前只有 XBTFUND FBR Second-Market 的比特币投资信托基金。参见 BTC。

[0484]XRP：XRP 也被称为 Ripple，是一个建立在区块链基础上的全球支付网络，在国际银行销售。Xrp 本身是昭应用程序可以用来表示平面货币、加密货币、商品或任何其他价值单位的原生货币。Ripple 是使用区块链的开放支付协议最古老的例子之一，但也有一长串公司拥有不同的 API、平台和分布式支付网络。德勤(Deloitte)的银行业展望最近发布了一份报告，估计到 2020 年，基于区块链的支付系统可能会与美国自动清算所(ACH)金融交易网络的规模相当。

Z。

[0485]零币：一种旨在使加密货币交易真正匿名的协议。

[0486]零确认交易：一种交易，在比特币的传输得到矿工确认并添加到区块链之前，商家很乐意提供产品或服务。它可能会带来重复支出的风险。

[0487]零确认交易：处理加密货币交易的数据可能需要半分钟以上的时间，在某些情况下可能需要十多分钟。虽然这对于验证交易是必要的，并防止重复支出等欺诈性活动，但等待时间可能会给参与交易的人带来不便。因此，一些与数字货币打交道的交易所和企业正在提供“零确认”交易，这些交易几乎可以立即得到验证，而无需等待 FBR 挖掘过程来确认数据块。重复消费，即硬币持有者将同一货币用于两笔不同的交易的做法，是零确认交易的一个令人担忧的问题。由于加密货币没有以任何方式“依附”于消费它的人，当他们的双重支出通过挖掘过程被发现时，他们早就不见了，无法追踪。随着 FBR 零确认交易需求的上升，加密货币行业的企业家们正在寻找立即验证或拒绝交易的方法，而不必等待 FBR 挖掘发生。与此同时，许多企业收取费用，以抵消零确认交易的财务风险，但还有一些企业拒绝接受这些费用，直到技术跟上。

[0488]Z 系统：IBM 公开承诺在许多方面推进区块链技术，但该公司甚至为 IBM Cloud 上的 FBR 开发人员提供了区块链即服务(Baas)平台，并在 IBM z Systems 上集成了基于区块链的应用程序(通过 Hyperledger 项目创建)。IBM 甚至计划在 Watson Lot 平台上利用区块链与 Watson 相结合，使来自基于 RFID 的位置、条形码扫描事件或设备报告的数据等设备的 FBR 信息能够与 IBM 的区块链一起使用，并与分布式分类账和智能合约同步。

我们声称：

1. 一种使用分布式分类帐的交易状态系统的系统 FBR 控制，包括：

应用平面层，所述应用平面层适于接收关于所述事务状态系统的操作的指令，所述应用平面层耦合到应用平面层接口，

控制平面层，所述控制平面层包括自适应控制单元，所述控制平面层经由所述应用平面层接口与所述应用平面层对接，以接收与关于所述交易状态系统的操作的指令有关的信息，以及。

数据平面层，所述数据平面层包括输入接口，以接收来自一个或多个数据源的数据输入，并提供耦合到分散分布式分类帐的输出，所述数据平面层耦合到所述控制平面层。

2. 如权利要求 1 所述的系统，其特征在于，所述系统控制事务状态系统，其中分散的分布式分类账存储关于加密货币的数据。

3. 如权利要求 1 所述的系统，其特征在于，所述自适应控制单元包括认知计算单元。

4. 如权利要求 1 所述的事务状态系统的系统 FBR 控制，其中所述控制平面层包括人工智能单元。

5. 如权利要求 1 所述的事务状态系统的系统 FBR 控制，其中所述控制平面层包括机器学习单元。

6. 如权利要求 1 所述的事务状态系统的系统 FBR 控制，其中所述控制平面层包括神经网络。

7. 如权利要求 6 所述的事务状态系统的系统 FBR 控制，其中所述神经网络是深度神经网络。

8. 如权利要求 6 所述的事务状态系统的系统 FBR 控制，其中所述神经网络包括图形处理单元(GPU)。

9. 如权利要求 6 所述的交易状态系统的系统 FBR 控制，其中所述神经网络是利用用户响应数据来训练的。

10. 如权利要求 6 所述的事务状态系统的系统 FBR 控制，其中所述神经网络是矢量化神经网络。

11. 如权利要求 6 所述的事务状态系统的系统 FBR 控制，其中所述神经网络是递归神经网络。

12. 如权利要求 1 所述的事务状态系统的系统 FBR 控制，其中所述控制计划层包括分析单元。

13. 根据权利要求 1 所述的事务状态系统的系统 FBR 控制，其中所述控制平面层还包括处理器。

14. 如权利要求 1 所述的事务状态系统的系统 FBR 控制，其中所述应用平面层包括图形用户界面单元。

15. 如权利要求 1 所述的事务状态系统的系统 FBR 控制，其中所述应用播放层还包括处理器。

16. 如权利要求 1 所述的事务状态系统的系统 FBR 控制，其中所述数据平面层包括输入端口。

17. 如权利要求 1 所述的事务状态系统的系统 FBR 控制，其中所述输入端口耦合以接收外部数据。

18. 根据权利要求 17 所述的交易状态系统的系统 FBR 控制，其中所述外部数据为物联网(Lot)数据。

19. 根据权利要求 17 所述的事务陈旧系统的系统 FBR 控制，其中所述输入端口耦合到处理器。

20. 如权利要求 1 所述的事务状态系统的系统 FBR 控制，其中所述数据平面层包括图形用户界面(GUI)生成器。

21. 如权利要求 20 所述的事务状态系统的系统 FBR 控制，其中所述图形用户界面耦合到输出端口。

22. 如权利要求 21 所述的事务状态系统的系统 FBR 控制，其中所述数据平面层包括适于耦合到显示设备的输出端口。

23. 如权利要求 1 所述的事务状态系统的系统 FBR 控制，其中所述数据平面层还包括值转移元件。

24. 如权利要求 1 所述的事务状态系统的系统 FBR 控制，其中所述数据平面层还包括标题转移元素。

25. 根据权利要求 1 所述的事务状态系统的系统 FBR 控制，其中所述数据平面层还包括管理网元。

26. 根据权利要求 1 所述的事务状态系统的系统 FBR 控制，其中所述数据平面层还包括控制网元。

US 20180373984A1

(19) **United States**
(12) **Patent Application Publication** (10) **Pub. No.: US 2018/0373984 A1**
KATZ et al. (43) **Pub. Date: Dec. 27, 2018**

(54) **ARCHITECTURES, SYSTEMS AND METHODS HAVING SEGREGATED SECURE FUNCTIONS AND PUBLIC FUNCTIONS**

(71) Applicant: **MILESTONE ENTERTAINMENT LLC**, Beverly Hills, CA (US)

(72) Inventors: **RANDALL M. KATZ**, Beverly Hills, CA (US); **ROBERT TERCEK**, Hollywood, CA (US)

(21) Appl. No.: **16/052,470**

(22) Filed: **Aug. 1, 2018**

Related U.S. Application Data

(63) Continuation of application No. 15/886,432, filed on Feb. 1, 2018.

(60) Provisional application No. 62/454,423, filed on Feb. 3, 2017.

Publication Classification

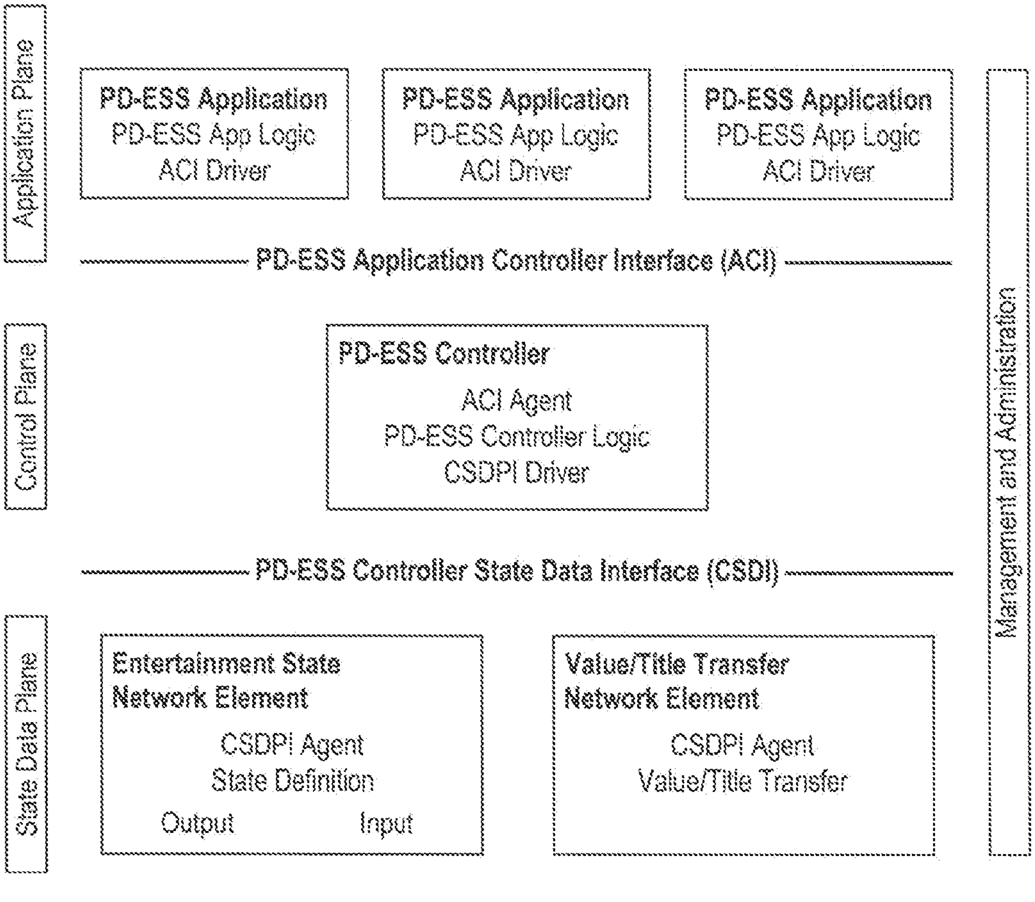
(51) **Int. Cl.**

G06N 3/08	(2006.01)
G07F 17/32	(2006.01)
G06K 9/00	(2006.01)
G06Q 20/06	(2006.01)

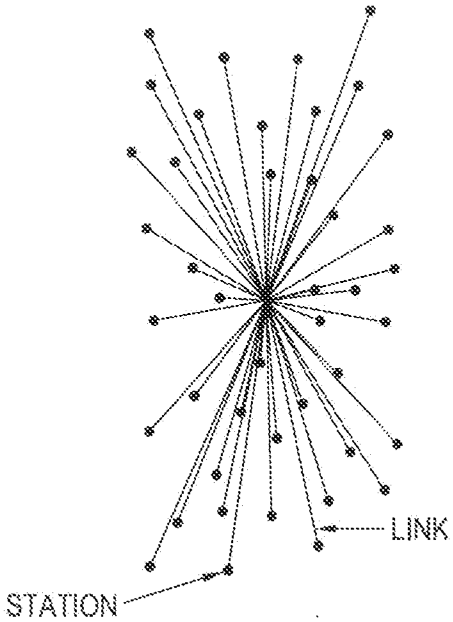
(52) **U.S. Cl.**
CPC *G06N 3/08* (2013.01); *G07F 17/329* (2013.01); *G06Q 20/065* (2013.01); *G06K 9/00221* (2013.01)

(57) **ABSTRACT**

A system is provided for control of an entertainment state system having segregated secure functions and public functions for use by one or more users of the system. First, a public interface portal receives instructions regarding operation of the entertainment state system from the one or more users. The interface portal includes a first interface, a processor, a graphical user interface (GUI) coupled to the processor, a control unit in operative communication with the processor and graphical user interface, and a second interface providing an application program interface (API). Secondly, a secure entity unit is provided, the secure entity unit including a receive interface, the receive interface adapted to receive a call from the application program interface (API) of the interface portal, a send interface, the send interface adapted to provide a response to the interface portal interface, a game engine, and a financial engine.



Programmatically Defined Gaming System

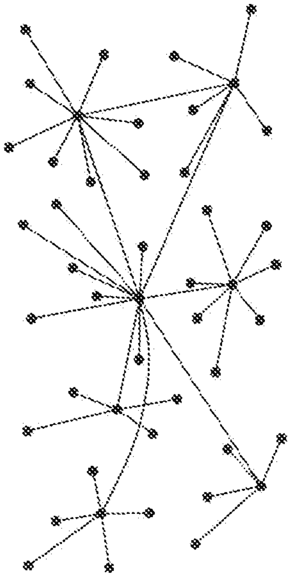


CENTRALIZED (A)

Prior Art Centralized System

FIG. 1

(Prior Art)

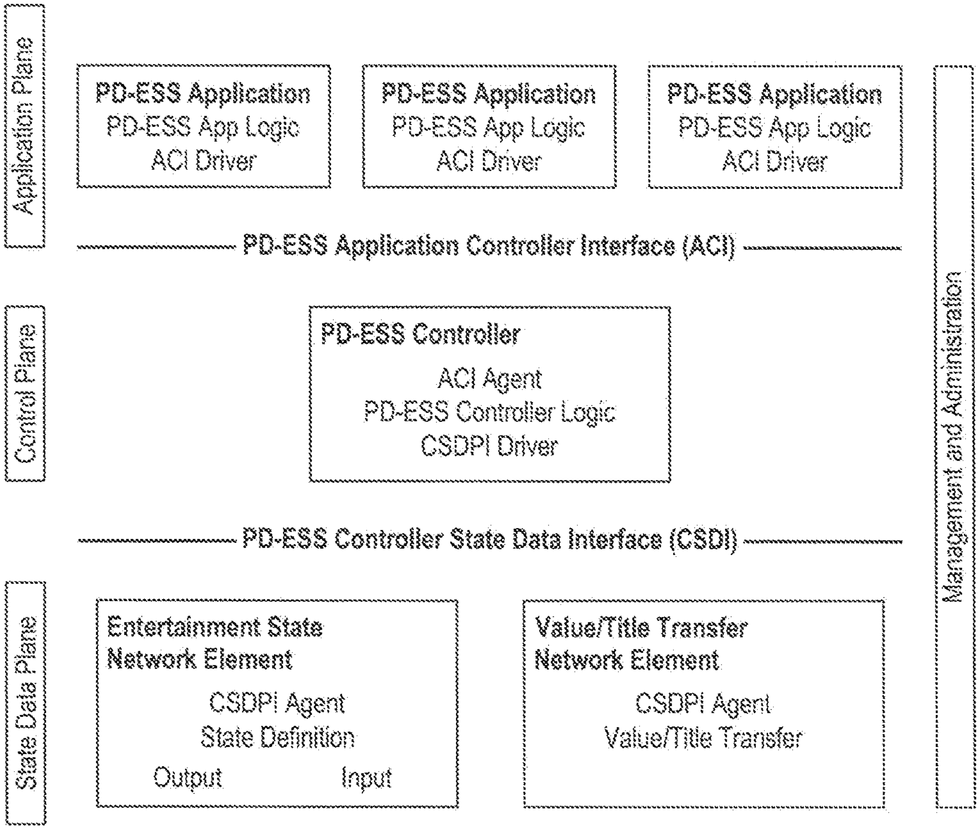


DECENTRALIZED

Prior Art Decentralized System

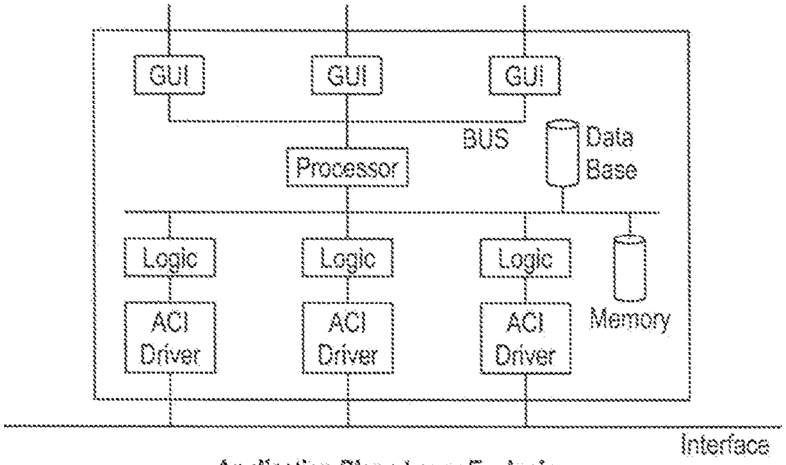
FIG. 2

(Prior Art)



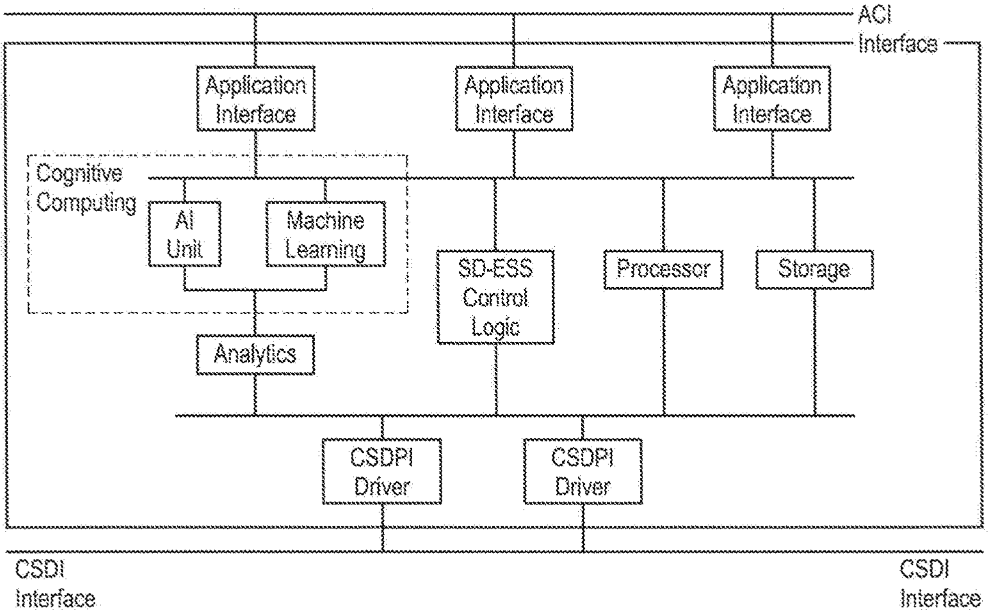
Programmatically Defined Gaming System

FIG. 3



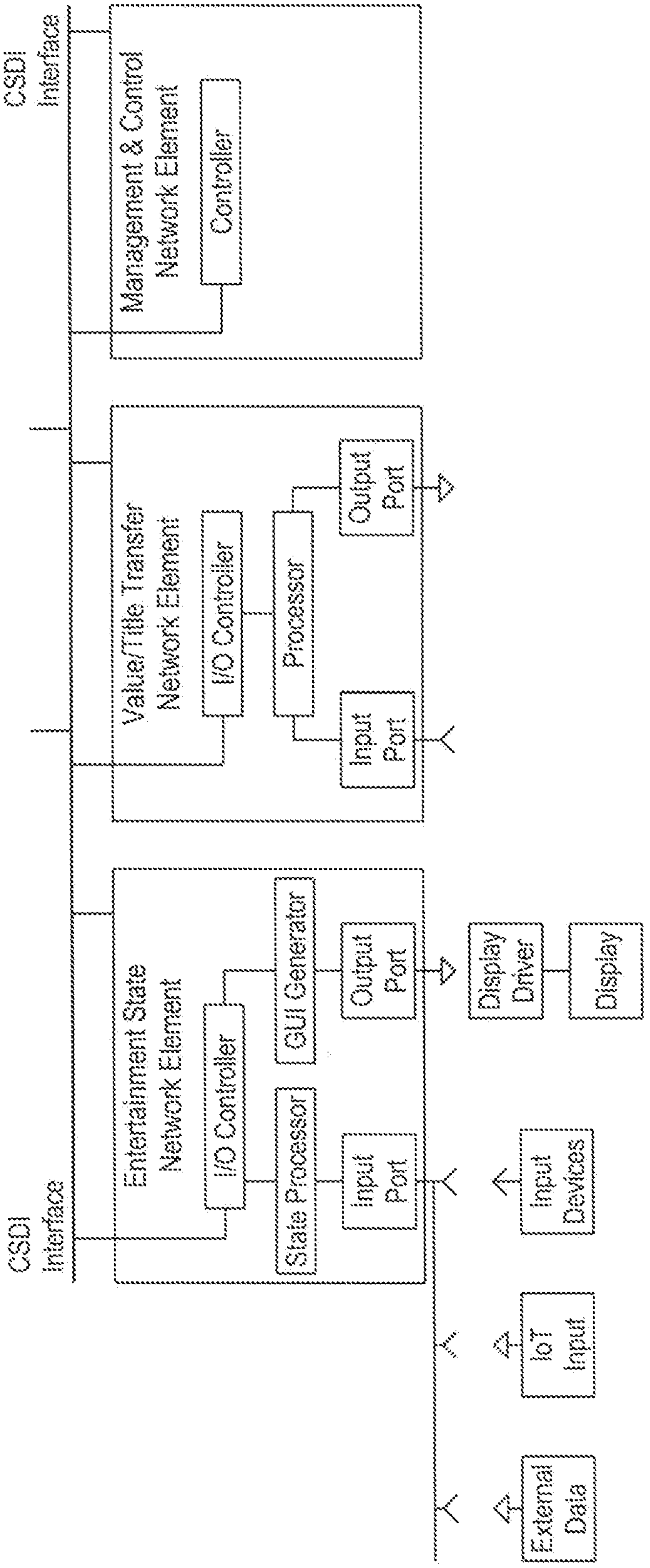
Application Plane Layer Explosion

FIG. 4



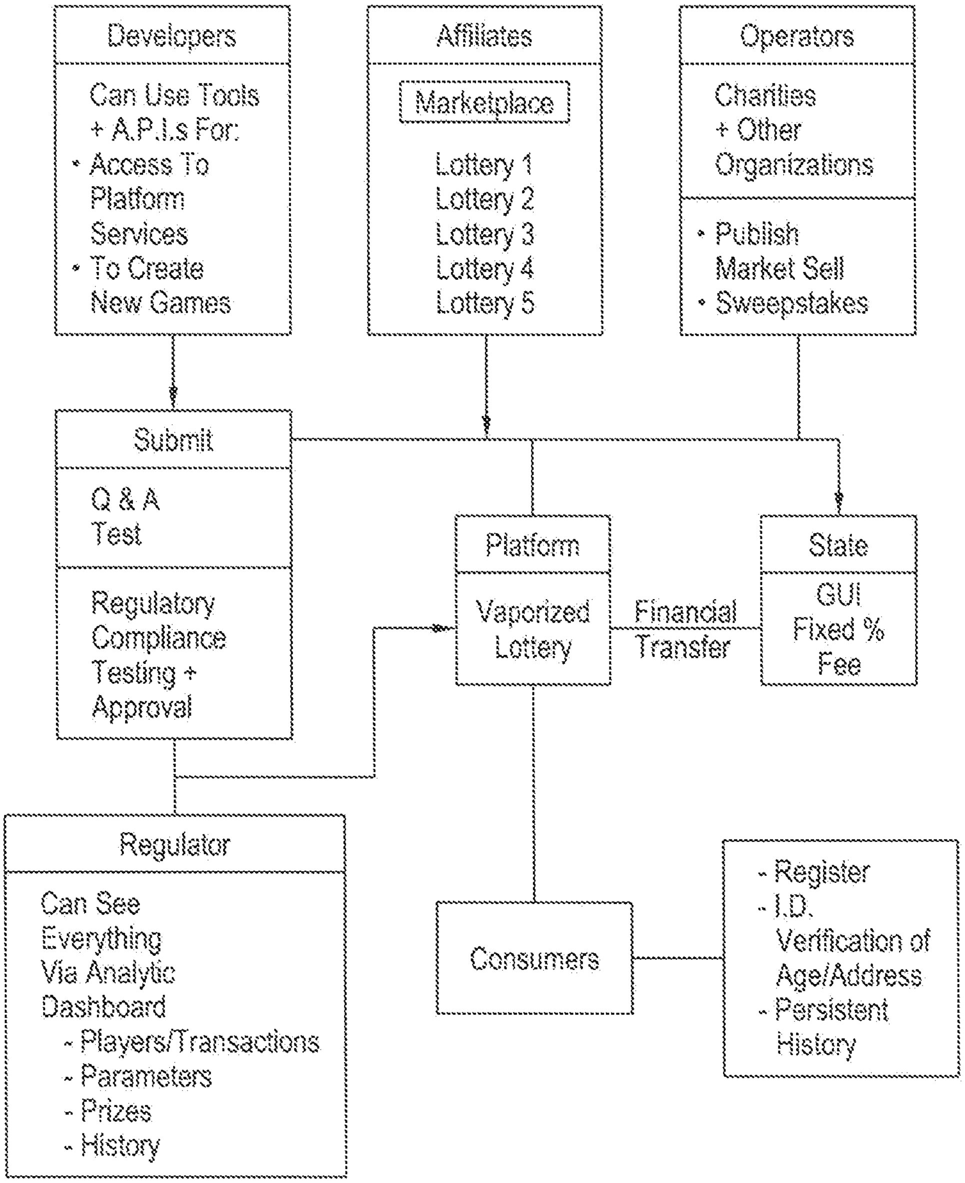
Control Plane Layer Explosion

FIG. 5



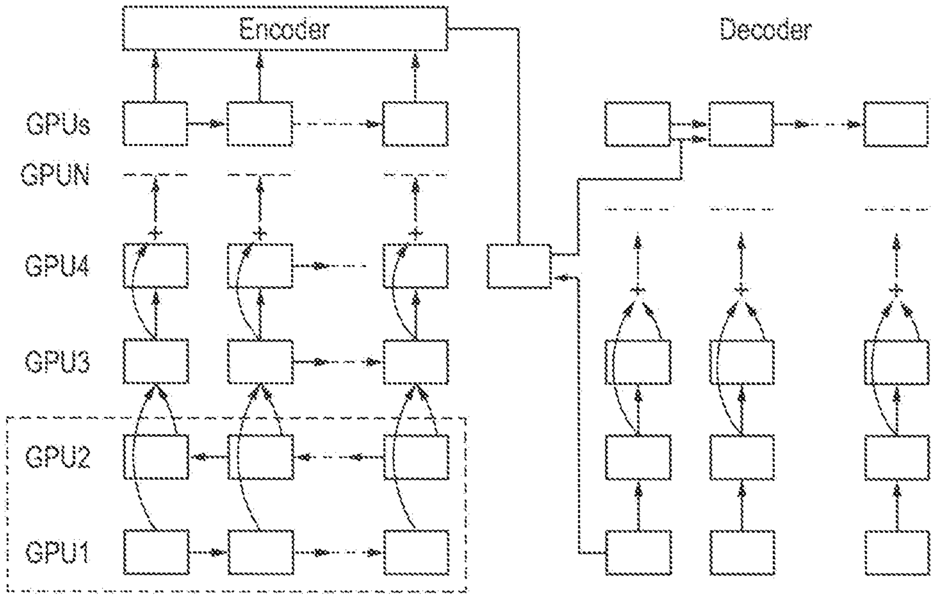
State Data Plane Layer Explosion

FIG. 6



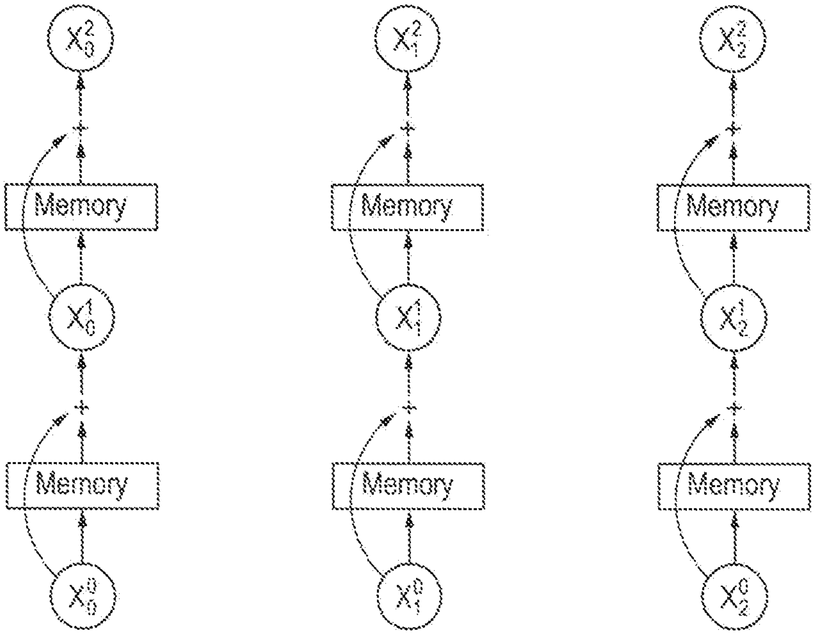
Ecosystem Interfaces and Interconnections

FIG. 7



Neural Network Model Architecture

FIG. 8



Neural Network

FIG. 9

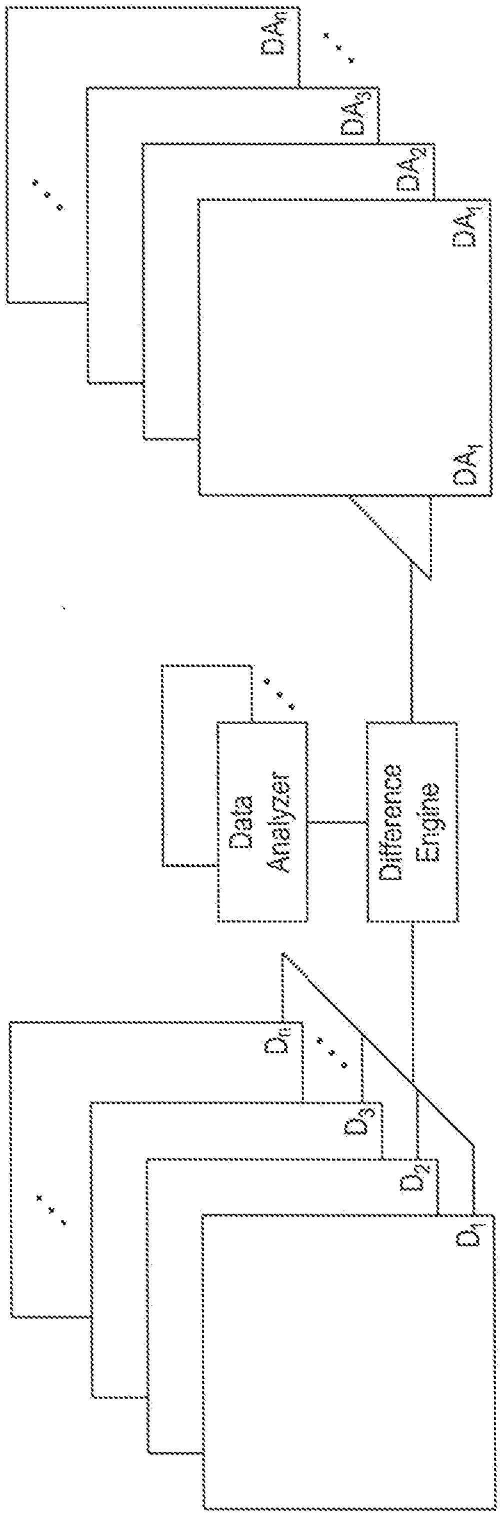

DA1
DA1
DA2
DA3
DAn
Data Analyzer
Difference Engine
D1
D2
D3
Dn

FIG. 10

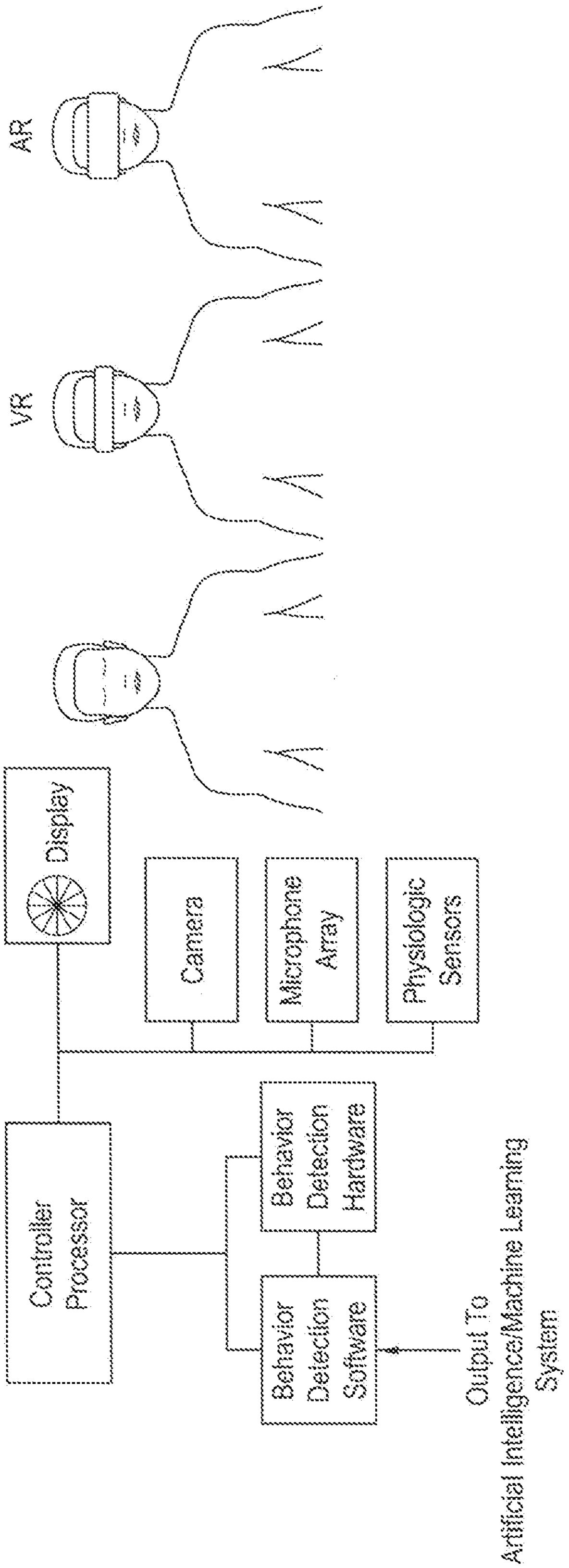
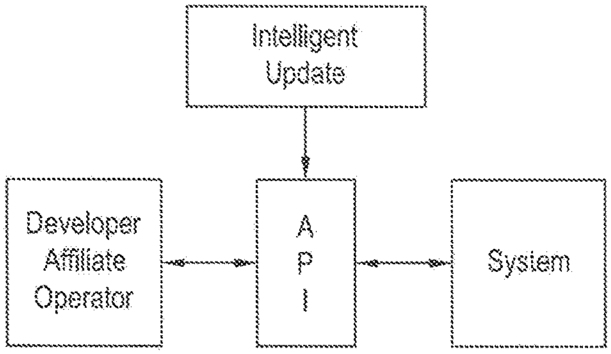
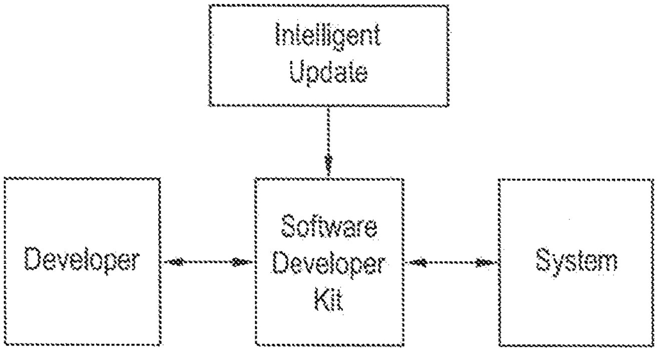

AR
VR
Display
Camera
Microphone Array
Physiologic Sensors
Controller Processor
Behavior Detection Hardware
Behavior Detection Software
Output To Artificial Intelligence/Machine Learning System

FIG. 11



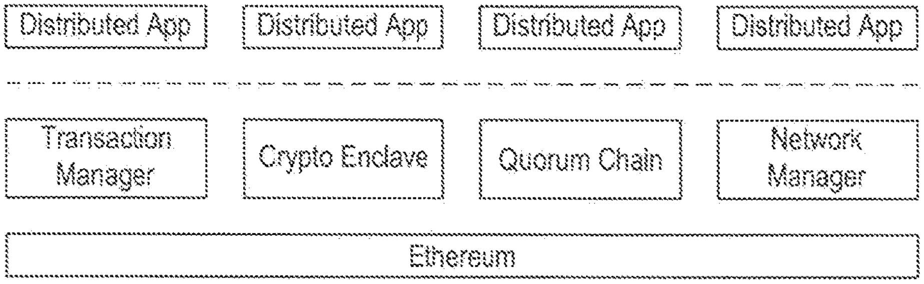
Dynamic Systems d-API

FIG. 12



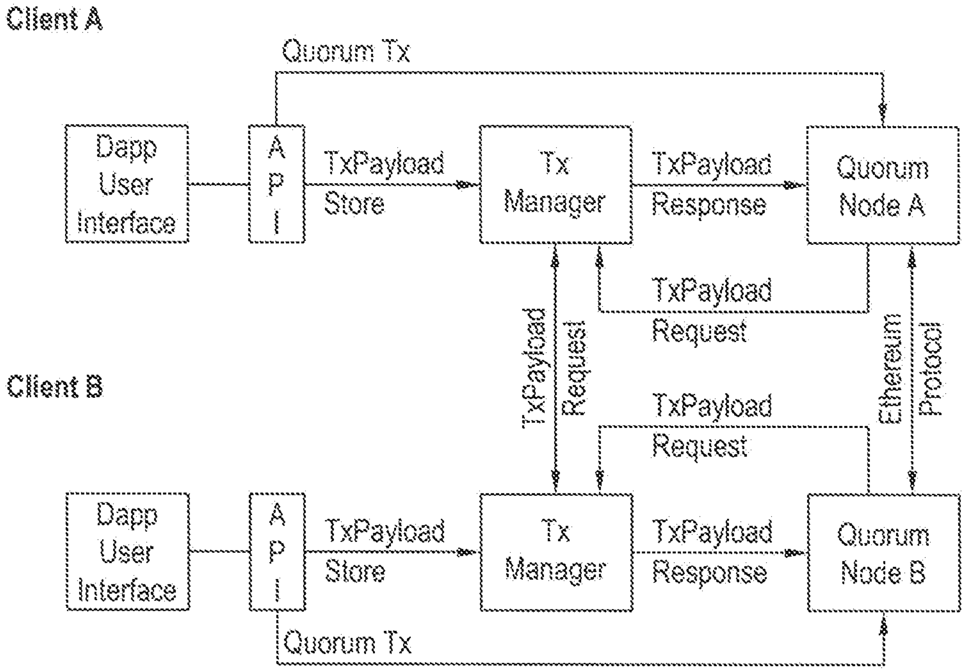
Dynamic Systems d-SDK

FIG. 13



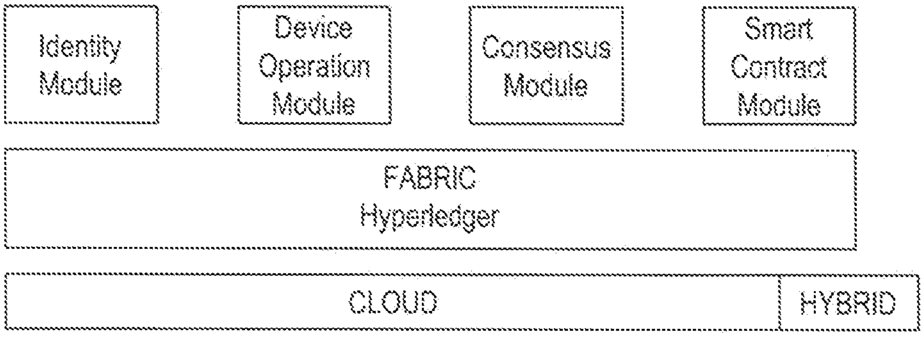
Architecture

FIG. 14



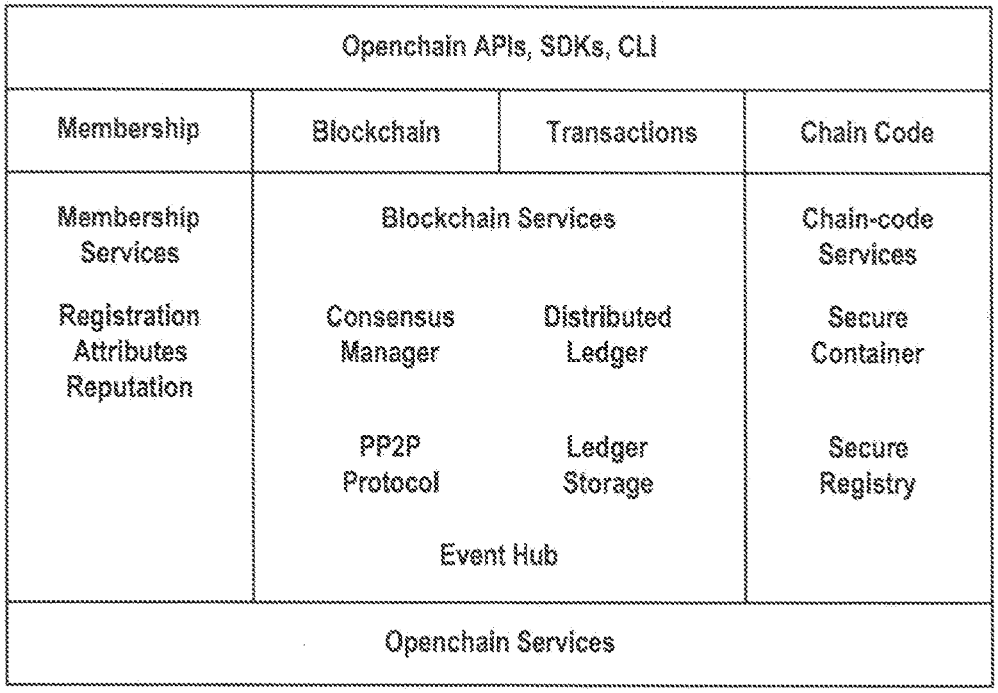
Permissioned System

FIG. 15



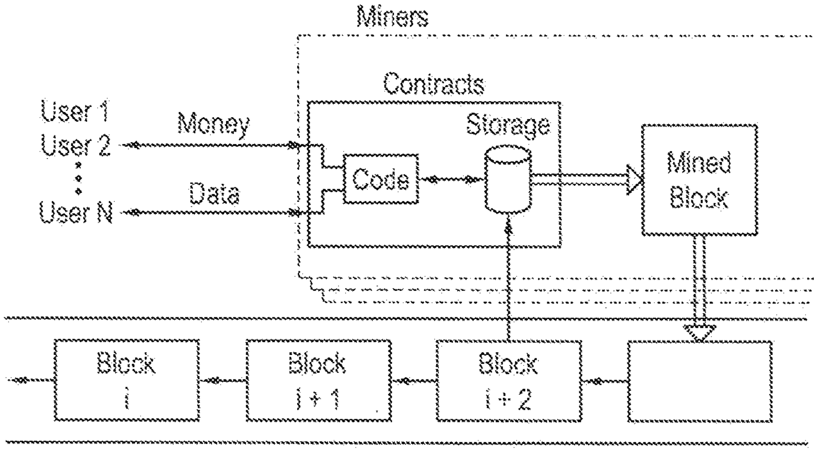
Blockchain Platform

FIG. 16



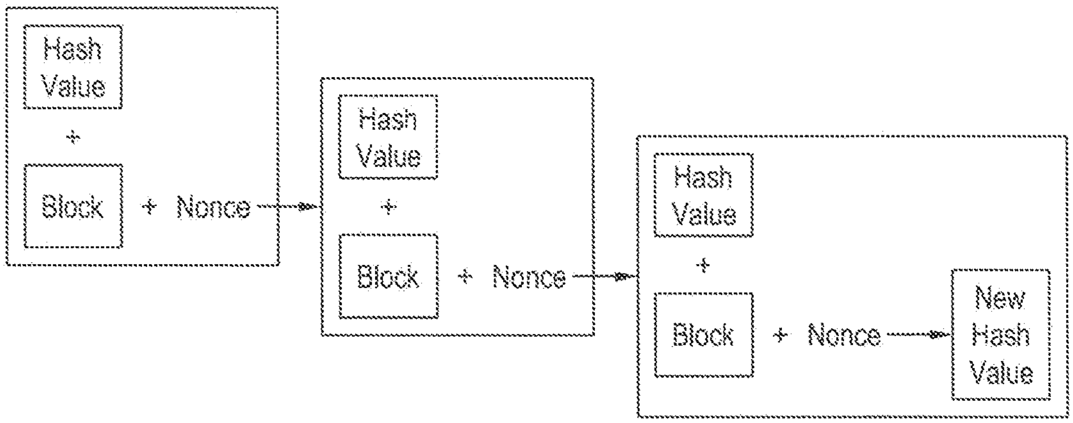
Platform

FIG. 17



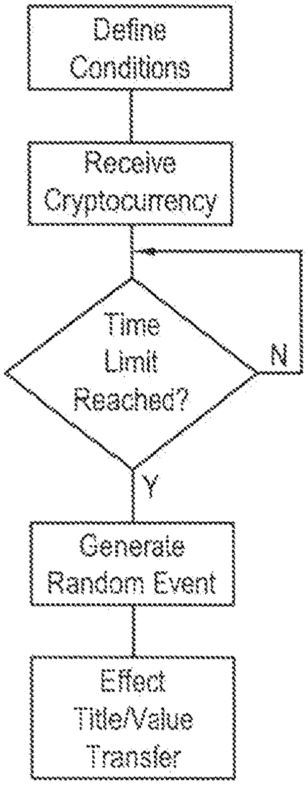
Schematic of a Decentralized Cryptocurrency System
with Smart Contracts

FIG. 18



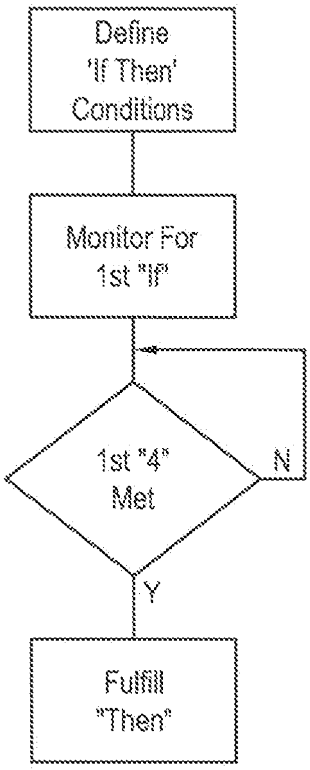
Schematic of Sequential Hash Value Creation
(Hash Value Plus Block Plus Nonce -> New Hash Value)

FIG. 19



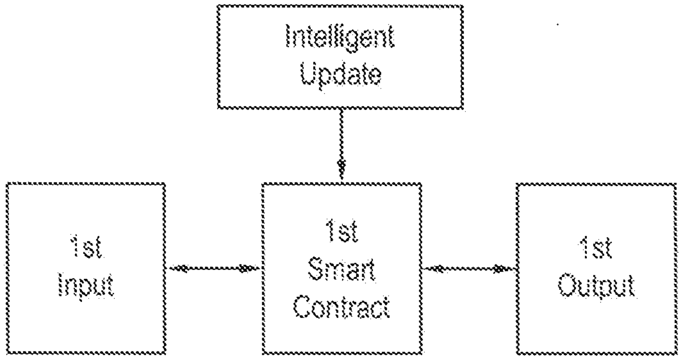
Flowchart for Crypto Currency Lottery

FIG. 20



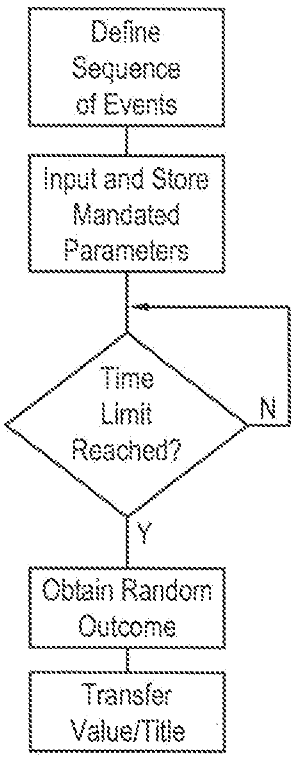
Smart Contract

FIG. 21



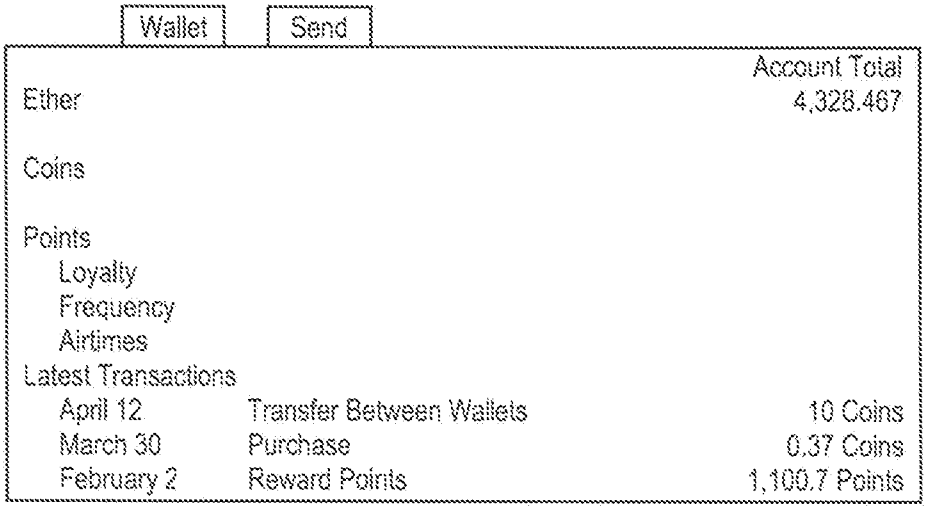
Smart-Smart (Smart^2) Contracts

FIG. 22



Smart Contracts with Mandated and Variable Parameters

FIG. 23



Account Total

Ether 4,328.467

Coins

Points

Loyalty

Frequency

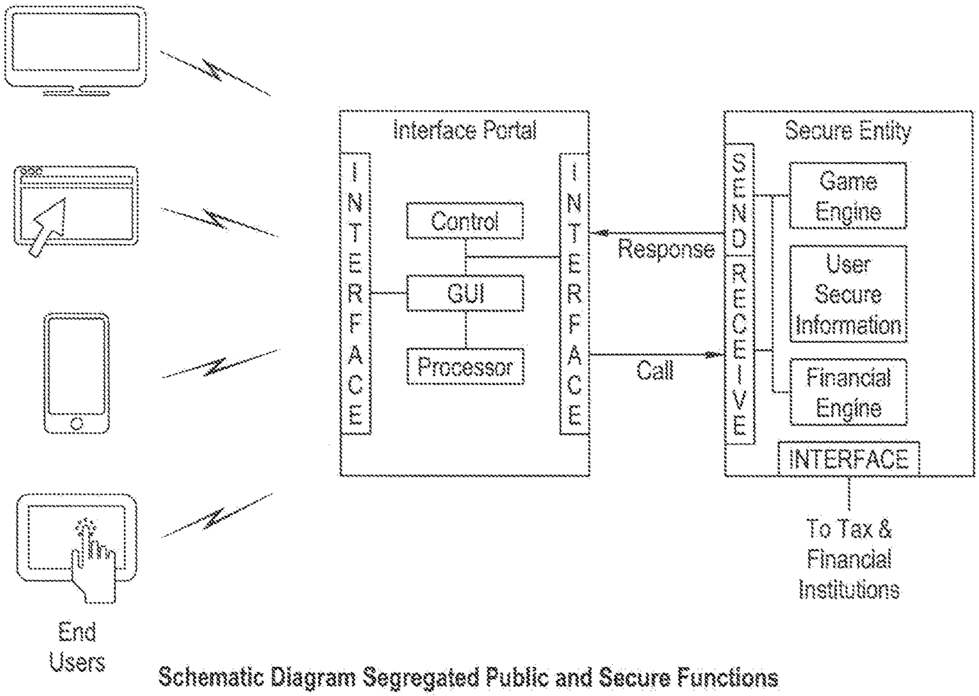
Airtimes

Latest Transactions

April 12	Transfer Between Wallets	10 Coins
March 30	Purchase	0.37 Coins
February 2	Reward Points	1,100.7 Points

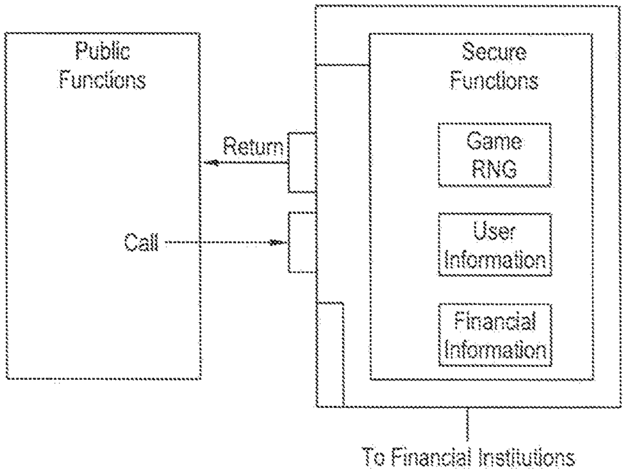
Cryptocurrency Wallet

FIG. 24



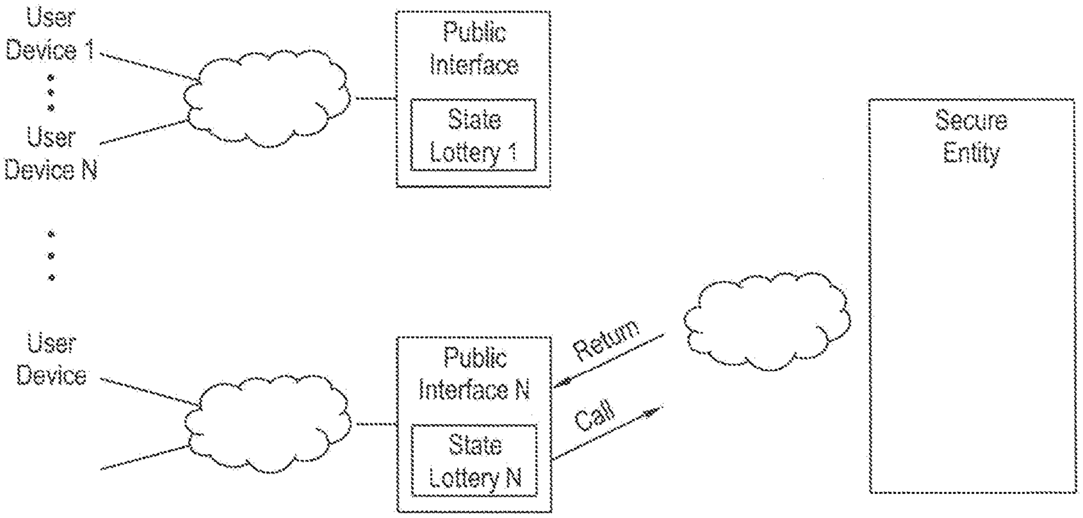
Schematic Diagram Segregated Public and Secure Functions

FIG. 25



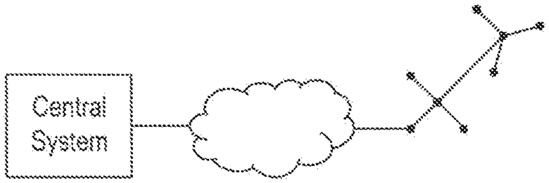
Interface of Segregated Secure and Public Functions

FIG. 26



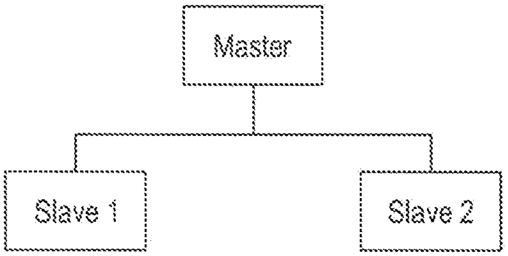
Network Implementation of Segregated Secure and Public Functions

FIG. 27



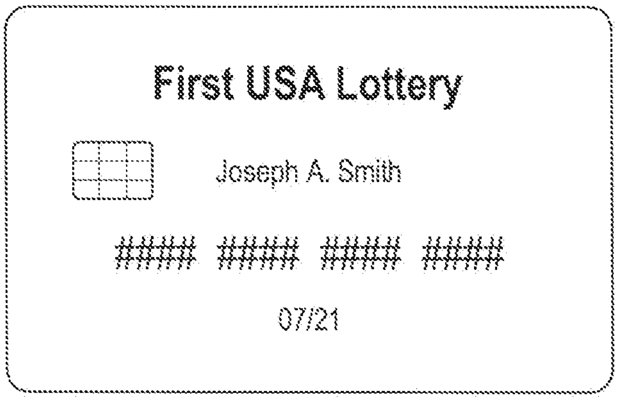
Centralized + Decentralized Systems

FIG. 28



Hierarchical Systems

FIG. 29



Lottery Linked Credit Card

FIG. 30

ARCHITECTURES, SYSTEMS AND METHODS HAVING SEGREGATED SECURE FUNCTIONS AND PUBLIC FUNCTIONS

PRIORITY CLAIM

[0001] This is a continuation of application Ser. No. 15/886,432, filed Feb. 1, 2018, which claims benefit of provisional Application No. 62/454,423, filed Feb. 3, 2017, which are incorporated herein by reference as if fully set forth herein.

FIELD OF THE INVENTION

[0002] The present inventions relate to architectures, systems and methods for programmatically controlled entertainment state systems. More particularly, architectures, systems and methods for program control utilizing cognitive computing, including but not limited to artificial intelligence and machine learning, and optionally including analytics. Systems, methods and architectures are provided for game and entertainment operations are provided utilizing decentralized systems, including blockchain, optionally in peer to peer systems. More particularly, systems and methods for implementing a lottery, game or entertainment utilizing cryptocurrency, such as bitcoin, in a decentralized system.

BACKGROUND OF THE INVENTION

[0003] History shows that many trusted systems have evolved in order to provide for efficient functioning of society and business. Generally, these have involved central control of systems in order to ensure compliance with rules. Within the gaming space, examples include lotteries and regulated gaming. By way of example, the Nevada Gaming Control Board monitors institutions within the state for compliance with laws and regulations, and ensures the fair and efficient functioning of the industry.

[0004] Consider the entertainment and gaming system background. A lottery is a 'State' Function and serves as a form of 'trusted agent'. The classic definition of the elements of a lottery are prize, chance and consideration. When these elements are reordered into a more chronologically correct order, namely first, receipt and holding of the consideration (e.g., ticket purchases), chance (e.g., ensuring a fair and accurate random number generator) and prize (i.e., paying the prize to the true winner.) Therefore, the State acts as a 'trusted agent' as it holds the consideration, guarantees randomness of the 'chance', and pays out the prize (title transfer). 'Trust' is based on the Integrity and Trustworthiness of People Operating the System and the Regulators Who Oversee the System. Lotteries or State Regulators are often former law enforcement. The degree of trust in the Regulators is often based on time and track record, e.g., the State of Nevada Regulatory system is considered highly trustworthy and effective, based in part on a multi-decade long track record. Additionally, a State with the most business to lose from a loss of trust in the regulatory process is most motivated to provide regulation. Such systems are based on central control of the system.

[0005] A casino is a 'state regulated' function and a form of 'trusted agent' with 'verification'. They are licensed by the State and subject to state inspection.

[0006] Various advancements have been made in the gaming and entertainment environment. The following are assigned to the assignee of this, and are hereby incorporated by Reference as if fully set forth herein: Games, And Methods For Improved Game Play In Games Of Chance And Games Of Skill, U.S. Pat. No. 6,565,084, Games, and Methods and Apparatus for Game Play in Games of Chance, U.S. Pat. No. 6,488,280, Games, and Methods and Apparatus for Game Play in Games of Chance, U.S. Pat. No. 6,811,484, Apparatus and Method for Game Play in an Electronic Environment, U.S. Pat. No. 8,393,946, Apparatus, Systems and Methods for Implementing Enhanced Gaming and Prizing Parameters in an Electronic Environment, U.S. Pat. No. 7,798,896, Apparatus, Systems and Methods for Implementing Enhanced Gaming and Prizing Parameters in an Electronic Environment, U.S. Pat. No. 8,241,110, Methods and Apparatus for Enhanced Play in Lottery and Gaming Environments, U.S. Pat. No. 8,727,853, Methods and Apparatus for Enhanced Interactive Game Play in Lottery and Gaming Environments. U.S. Pat. No. 8,241,100, Method and System for Electronic Interaction In A Multi-Player Gaming System, U.S. Pat. No. 8,535,134. Generally, they comprise a suite of tools to make systems more engaging, and to optimize results.

[0007] One vexing problem in larger systems results from systems incompatibility. Various components often come from various vendors. There is often a lack of interoperability and incompatibility. Various systems in the gaming ecosystem need to interoperate, including but not limited to: gaming operations, marketing, CRM (Customer Relationship Management), loyalty programs, Ancillary Points or Credits, System Analytics and Optimization, and account and audit functions.

[0008] Software Defined Systems are a collection of modules interoperated under a higher level of software control. These manage network services through abstraction of lower level functionality. Generally, there is an Application Plane, a Control Plane and a Data Plane. Examples include Software Defined Networks having a Control Plane which provides intelligent control of data plane composed of relatively less intelligent switches, routers, storage. Yet another example is software defined radio. The control plane monitors and supervises use of frequency bands in the data plane.

[0009] Yet another component is the use of static interfaces and tools. For example, APIs or Application Programming Interfaces generally comprise a static interface. They define a format for an information request. 'If you ask for X in a specific way, we will provide Y'. Generally, no access is provided by requestor to the system other than via API. Yet another system are SDKs or Software Development Kit. They may be static. Tools are provided to achieve desired results. GDKs or Game Development Kit also may be static and provide tools for game development.

[0010] The design of entertainment or games is often driven by metrics driven design. This often involves A/B Testing comparing the results or favorability as between multiple systems. Further, they often monitor multivariate response systems.

[0011] One aspect of lotteries and Lotto style games is that they tend to be static. At the most extreme example, they are literally printed on cardstock. More generally, once a format for a lottery game has been chosen, such as a 6 out of 49 format, it is difficult to change. Public perception of change is that the game has become less favorable to the player.

[0012] Problem gambling issues have plagued the gaming industry. It is a significant issue for society. While users can solicit help (e.g., 1-800-Gambling), there is often denial and an unwillingness to seek help. Various attempts have been made to limit abuse, such as use rate limits in some on-line games.

[0013] In the move from bricks and mortar to on-line and cyber spheres, identity issues proliferate. Issues include: are you who you purport to be and will the user's identity be compromised?

[0014] Significant advances have been made in cognitive intelligence and adaptive intelligence. For example, IBM Watson won a Jeopardy competition 2011 against highly skilled players. Deep learning and pattern recognition has occurred. Current trends include big data, pattern recognition and machine learning.

[0015] Recent advances have also been made in object detection, both in 2D and 3D space. A challenge in the Large Scale Visual Recognition Challenge (LSVRC) provides for Object Detection in ImageNet 2016. The error rate of automatic labeling of ImageNet declined to less than 3%, compared to human performance of about 5%.

[0016] Significant advances have also been made in machine based game play performance. In 2015, Google DeepMind used an artificial intelligence reinforcement learning system to learn how to play 49 Atari games. In 2016, AlphaGo system from Google DeepMind beat one of the world's greatest Go players 4-1. In 2017, Carnegie Mellon University's Libratus program defeated top human players in a statistically significant manner.

[0017] Further advances have been made in cloud based systems. Functions have been migrating from local servers and storage to remote 'cloud' storage. These systems provide for easy scalability. Clouds based systems may run multiple 'instances' simultaneously. They also may combine software as a service, including Artificial Intelligence ("AI").

[0018] The Internet of Things ("IoT") utilizes devices capable of sending data to remote location, and receiving command data. Various voice controlled devices use AI or machine learning ("ML"), e.g., Amazon Alexa, Google Dot.

[0019] FIG. **1** shows an exemplary prior art centralized system. FIG. **2** shows an exemplary prior art distributed system.

[0020] Advancements have been made in trusted distributed systems such as in the use of blockchain based systems. The initial disclosure of the blockchain technology is attributed to Satoshi Nakamoto in a paper published October, 2008. This system provides for automatic trust or system trust. The blockchain paradigm provides for a decentralized system utilizing decentralized consensus. This can be done in a peer-to-peer manner without an intermediary. The system may be viewed as a network of nodes running software on a programmable distributed network. It is sometimes referred to as a transaction singleton machine with shared state, a transaction based state machine, a message passing framework, a trustful object messaging compute framework and trusted computing.

[0021] A decentralized consensus is established by a combination of blockchain and cryptography. Authority and trust is provided by the decentralized virtual network. Consensus logic is generally separate from the application. It may comprise the first layer of a decentralized architecture.

[0022] Blockchain utilizes a distributed ledger. A 'block' comprises a new group of accepted transactions. A batch of transactions is released in a block to be validated by the network of participating computers. Continuous, sequential transaction record on a public block creates a unique "chain" or blockchain. This block is published to all other nodes. The publication occurs periodically, e.g. every 10 minutes.

[0023] Etherium is an open source platform for smart contracts. As currently operated, Etherium is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference. The applications run on a custom built blockchain, an extremely powerful shared global infrastructure that can move the value and represent ownership of the property. This allows developers to create markets, store debt or promise records, move funds according to long-standing instructions (such as a will or a futures contract), without the counterparty risk. Etherium also states that its goal is to create a tradeable digital token that can be used as a currency, a representation of an asset, a virtual share, a proof of membership or anything at all. These tokens use a standard coin API, so the contract will be automatically compatible with any wallet, other contract or exchange also using this standard. The total amount of tokens in circulation can be set to a simple fixed amount or fluctuate based on any programmed ruleset. In summary, Etherium states that it enables building a tradeable token with a fixed supply, a central bank that can issue money and a puzzle-based cryptocurrency.

[0024] There are many disadvantages to the current systems. They are slow to change and innovate. They often involve proprietary systems that do not interoperate. There is often governmental and or institutional bias. There may be a cumbersome regulatory environment. Finally, there are often high transaction costs.

[0025] Thus, there is a need for interoperability among inconsistent, often proprietary systems. There is a need for gambling limitation on a more global basis, including geo-limitation and global use rate monitoring for problem gambling. There is a need for problem gambling detection and remediation. There is a need for improved distributed systems.

SUMMARY OF THE INVENTION

[0026] In one aspect, the inventions comprise a system for control of an entertainment state system having segregated secure functions and public functions for use by one or more users of the system. First, a public interface portal receives instructions regarding operation of the entertainment state system from the one or more users. The interface portal includes a first interface to receive instructions from and communicate to the one or more end users, a processor, a graphical user interface (GUI) coupled to the processor, a control unit in operative communication with the processor and graphical user interface, and a second interface providing an application program interface (API). Secondly, a secure entity unit is provided, the secure entity unit including a receive interface, the receive interface adapted to receive a call from the application program interface (API) of the interface portal, a send interface, the send interface adapted to provide a response to the interface portal interface, a game engine, and a financial engine. Preferably the financial engine is coupled to the game engine, the receive interface and the send interface.

[0027] Systems and methods are provided for training an artificial intelligence system including the use of one or more human subject responses to stimuli as input to the artificial intelligence system. One or more displays are oriented toward the human subjects to present the stimuli to the human subjects. One or more detectors serve to monitor the reaction of the human subjects to the stimuli, the detectors including at least motion detectors, the detectors providing an output. An analysis system is coupled to receive the output of the detectors, the analysis system providing an output corresponding to whether the reaction of the human subjects was positive or negative. A neural network utilizes the output of the analysis system to provide a positive weighting for training of the neural network when the output of the analysis system was positive, and a negative weighting for training of the neural network when the output of the analysis system was negative.

BRIEF DESCRIPTION OF THE DRAWINGS

[0028] FIG. **1** is a diagrammatic view of a prior art centralized system.

[0029] FIG. **2** is a diagrammatic view of a prior art centralized system.

[0030] FIG. **3** is a system level block diagram of the program defined entertainment state system (PD-ESS) showing the application plane, the control plane and the state data plane.

[0031] FIG. **4** is a system level block diagram explosion of the application state plane layer of the PD-ESS.

[0032] FIG. **5** is a system level block diagram explosion of the control plane layer of the PD-ESS.

[0033] FIG. **6** is a system level block diagram explosion of the state data plane layer of the PD-ESS.

[0034] FIG. **7** is a diagrammatic view of the ecosystem, including interfaces and interconnections.

[0035] FIG. **8** is a system level block diagram of the neural network model architecture including graphical processing units (GPUs).

[0036] FIG. **9** is a system level block diagram of the neural network model architecture.

[0037] FIG. **10** is a system level diagram of multiple data sets including a difference engine and data analyzer.

[0038] FIG. **11** is response system display and detection system for generating input to train the artificial intelligence (AI) and machine learning (ML) systems.

[0039] FIG. **12** is a system level diagram of a dynamic system application programming interface (d-API).

[0040] FIG. **13** is a system level diagram of a dynamic software development kit (d-SDK).

[0041] FIG. **14** is a system architecture level diagram of a distributed system including blockchain and Etherium.

[0042] FIG. **15** is a system architecture level diagram of a permissioned blockchain system.

[0043] FIG. **16** is a system architecture level diagram of a blockchain platform.

[0044] FIG. **17** is a system architecture level diagram of a blockchain platform including open chain services.

[0045] FIG. **18** is a system architecture level diagram of a decentralized cryptocurrency system with smart contracts.

[0046] FIG. **19** is a system architecture level diagram of a decentralized system with sequential hash value creation.

[0047] FIG. **20** is a flowchart diagram of a cryptocurrency lottery.

[0048] FIG. **21** is a flowchart diagram of a smart contract.

[0049] FIG. **22** is a flowchart diagram of a smart-smart (smart^2) contract.

[0050] FIG. **23** is a flowchart diagram of a smart contract having mandated and variable parameters.

[0051] FIG. **24** is a graphical user interface (GUI) of a cryptocurrency wallet.

[0052] FIG. **25** is a system architecture level schematic diagram of a system having segregated public and secure functions.

[0053] FIG. **26** is a system architecture level of an interface of segregated public and secure functions.

[0054] FIG. **27** is a system architecture level of a network implementation of a system having segregated public and secure functions.

[0055] FIG. **28** is a system architecture level of a combined centralized and decentralized system.

[0056] FIG. **29** is a system architecture level of a hierarchical system.

[0057] FIG. **30** is a plan view of a lottery linked credit card.

DETAILED DESCRIPTION OF THE INVENTION

[0058] Architectures, Systems and Methods for Program Defined Entertainment State Systems.

[0059] The following description is primarily in connection with FIGS. **3**, **4**, **5** and **6**, but may apply to other figures as well. An architecture is provided for a program defined entertainment state system. This preferably serves to decouple the system that controls the overall experience from the underlying systems that define states. The first plane, the application plane provides an interface, primarily for system side users, e.g., developers, organizers of events, contests, lotteries. The second plane, the control plane, provides for intelligent control, especially cognitive computing, including artificial intelligence and/or machine learning, including artificial intelligence where the system learns over time. This preferably provides an intelligent control layer above modules. The third plane, the state data plane, provides for entertainment 'state modules' with various mechanics, preferably including 'core loop', meta states and provides interfaces for end users, as well as inputs and outputs.

[0060] FIG. **3** provides a block Diagram Program Defined Entertainment State System (PD-ESS). FIG. **4** is an Explosion of PD-ESS Application Plane Layer, including an application layer GUI (facing the Developers, Affiliates, and Charities). FIG. **5** provides an Explosion PD-ESS controller plane layer. FIG. **6** provides an explosion PD-ESS state data plane layer. Also included are an explosion of entertainment state network element layer, a user interface GUI, an explosion of value/title transfer network element and explosion of other functional blocks.

[0061] Turning first to the Application Plane layer, a program serves to communicate requirements and desired behavior to the PD-ESS Controller. It provides communication between the PD-ESS Application and PD-ESS Controller via the PD-ESS Application Controller Interface (ACI). Application Logic and Drivers are optionally provided. The application layer may receive an abstracted view of State Data Plane Actions. The PD-ESS Applications may interface with higher levels of abstracted control. The system includes an interface, the PD-ESS Application Controller Interface (ACI). The management and administration preferably provides the following: (1) To/From Application Plane, it provides contracts and SLAs, (2) To/from Control

Plane Configure Policy, Monitor Performance, and (3) To/From Data Plane Element Setup.

[0062] Turning second to the Control Plane Layer, the PD-ESS Controller is ideally logically centralized entity, preferably serves to translate the requirements of the PD-ESS Application to the State Data Plane layer, and provides the Application layer with actions in the State Data Plane (e.g., event information and statistical information). The control plane may provide statistics, events and states from the Data Plane to the Application Plane. The control plane preferably enforces behavior at a low level control in the data plane, provides capability discovery, and monitors statistics and faults. The control plane advantageously includes cognitive computing, such as artificial intelligence (AI) and machine learning (ML), to be described in greater detail, below.

[0063] The control plane may optionally include analytics, including but not limited to pattern recognition. Analytics may be performed on a population, preferably a relevant population, or on a subset. Preferably, the subset has similar characteristics of a target user. Data may be binned according to subset. The scope of primary data may be analyzed. Predictive modeling may be included. Responsible Gaming Control may be implemented at the control plane level, especially if there are use rate limits and global limits.

[0064] Turning thirdly to the state data plane layer, it preferably includes main subcomponents and Functional Network Elements. Optionally, the functional network elements include some or all of the following: 1. Entertainment State Network Elements, 2. Value/Title Transfer Network Element, 3. Game Library, such as Casino, VLT, Video Gaming, Tournament, Amusement with Prize (AWP), Game Mechanics, Core Loop, Skill, Skill with Reveal, Second Chance, Social, Gamification, Prizing, vGLEPs and Prize Board, 4. Systems, Marketing, Promotions, CRM, Operations, Logistics, Interactive, Mobile/Apps and Responsive Design, 5. Platforms, 6. Channels, 7. Lottery, including Retail and Central Systems, 8. Loyalty, 9. Responsible Gaming Control, optionally including use rate limits and global limits (may be done in the control plane layer as well), 10. Sports, including real world, fantasy and eSports, 11. Other Live Data Entertainment, 12. Networks, including Network communications and web services and 13. Management, including Records, Player Account Management, Reporting, Compliance, including regulatory compliance, security, including cybersecurity, fraud and risk management, including preferably audit and payment.

[0065] The Entertainment State Network Elements provide an interface for interaction with a user of the system. An input receives information from user selection. Sensors may be of various forms, including sound sensors, motion sensors, whether 2-d or 3-d, such as including the Microsoft Kinect system. 'Internal Data' consists of data related primarily to game operations. 'External' Data sources to combine with Primary Data Source. These may include 1. Location, 2. Current Activity such as Driving (provided by vehicle, provided by tracked phone) or Exercising (provided by FitBit or similar), 3. Economic Conditions, 4. Weather, 5. Recent Events/News, e.g., a recent Large PowerBall win, 6. Marketing Information, 7. e-mail scans, e.g., Google scanning of Gmail for content, 8. Social Media, and 9. the Internet of Things (IoT). The Internet of Things (IoT) provide various forms of connected devices such as data sensors. The sensors generate data input "stimuli" to system. By utilizing any form of input, the system is able to provide for massive parallelism. All data "stimuli" to system permits the system to be adaptive and reactive to all data stimuli.

[0066] An Output provides stimulation to user. Forms may include: 1. images, such on a display, or via a GUI, or VR system, AR system, 2. Thin Client display with remote computing power, 3. Projections and Holograms, 4. sounds, 5. tactile stimuli, 6. olfactory stimuli, or 7. direct electrical stimuli, neural or otherwise.

[0067] A Value/Title Transfer Network Element serves to receive and transfer value (money, coins, and other items of value). Value may refer to fungible liquid asset or other store of value. Title generally refers to ownership of real, personal, or virtual property. A detailed discussion of blockchain, trust-less, and cryptocurrency systems is provided, below.

[0068] Artificial Intelligence (AI) is broadly that branch of computer science dealing in automating intelligent behavior. They are systems whose objective is to use machines to emulate and simulate human intelligence and corresponding behavior. This may take many forms, including symbolic or symbol manipulation AI. It may address analyzing abstract symbols and/or human readable symbols. It may form abstract connections between data or other information or stimuli. It may form logical conclusions. Artificial intelligence is the intelligence exhibited by machines, programs or software. It is has been defined as the study and design of intelligent agents, in which an intelligent agent is a system that perceives its environment and takes actions that maximize its chances of success. Yet others have defined it as the science and engineering of making intelligent machines.

[0069] Artificial Intelligence often involves use of neural networks. In various embodiments, a multi-layer stack of neural network nodes are utilized. The lowest level comprises granular elements. By way of example in a gaming application, in the order of higher level understanding, the levels would progress from instances of individual action (granular), to core loop detection, to session play, to multi-session play. Optionally, a parsing engine serves to break down or subdivide a larger set, such as a data set or image, into more discrete or granular elements.

[0070] AI may have various attributes. It may have deduction, reasoning, and problem solving. It may include knowledge representation or learning. Systems may perform natural language processing (communication). Yet others perform perception, motion detection and information manipulation. At higher levels of abstraction, it may result in social intelligence, creativity and general intelligence. Various approaches are employed including cybernetics and brain simulation, symbolic, sub-symbolic, and statistical, as well as integrating the approaches.

[0071] Various tools may be employed, either alone or in combinations. They include search and optimization, logic, probabilistic methods for uncertain reasoning, classifiers and statistical learning methods, neural networks, deep feedforward neural networks, deep recurrent neural networks, deep learning, control theory and languages.

[0072] AI advantageously utilizes parallel processing and even massively parallel processing in their architectures. Graphics Processing Units (GPUs) provide for parallel processing. Current versions of GPUs are available from various sources, e.g., Nvidia, Nervana Systems.

[0073] Machine Learning is defined as a system that builds up knowledge from experience. Machine learning serves to detect patterns and laws.

[0074] Deep Learning uses Neural AI. It is easily scalable, and typically involves more layers or neural Networks (NNs). Neural Networks may be of various forms, including: efficient NN, vectorized NN, vectorized logistic regression, vectorized logistic regression gradient output, binary classification, logistic regression, logistic regression cost function, gradient descent, derivatives, computation graph and logistic regression gradient descent.

[0075] Deep neural networks (DNN) often involve hyperparameter tuning. Typically they utilize regularization and optimization. Sometimes they are referred to as Deep Belief Network (DBN).

[0076] Other forms of neural networks include Convolutional Neural Networks (CNN) or Recurrent Neural Networks (RNN). Examples of available systems include: LSTM, Adam, Caffe, Dropout, Batch Norm, Xavier/He, Python, Scikit-Learn and TensorFlow.

[0077] AI may operate on various forms of data sets. The data set may comprise images, whether video images, 2D Data and/or 3D Data. Sequential data may be analyzed. Examples include, but are not limited to, natural language, audio, autonomous driving decisions, game states and game decisions.

[0078] Various industry applications advantageously benefit from application of AI. They include imaging and object detecting, serving to identify, classify, mining and optionally provide sentiment analysis. Other applications include autonomous driving. Yet other applications include robots and robotics. Within healthcare, functions include imaging analysis, diagnosing and gamification. Various forms of sequential data analysis may be enhanced, such as speech recognition, and natural language processing. Music applications include both recognition and synthesis. Within the gaming field, applications include game state sequences detection, analysis, formation, combination optimization, and game optimization. Chat bots and machine translation advantageously employ these systems.

[0079] FIG. **7** shows the constituent function blocks within an entertainment or gaming ecosystem. Affiliates serve to acquire customers. Affiliates receive a commission, such as based on the number of users acquired or a percent (%) of revenue. Optionally, there is a link to a credit card function (to be discussed, below in connection with FIG. **30**).

[0080] Next are charities and other organizations that plan to operate a lottery, game or other entertainment event. They provide for customer acquisitions. They are the recipient of the event (game, lottery or entertainment). They also collect a fee.

[0081] Next are the developers, who provide for game design. In return for game design, they receive multi-jurisdictional use and payment for use. An enhanced application or app store may be provided wherein the game design may be viewed, selected and downloaded.

[0082] Next, consumers provide registration and identification information. The registration data may optionally include identification, age, address and verification. Optionally, the data is sufficient that the system can comply with Know Your Customer (KYC) rules, with optional levels of identity verification. This is stored as persistent history. The customer receives a chance to play, win, and receive entertainment.

[0083] Next is the regulator or trust verifying agent. They provide testing, approval for game fairness, overall approval, ensure compliance with regulations and security. The regulator or trust verifying agent is granted access permission by the system to monitoring of every transaction, (analytics dashboard), player accounts, parameters, prize amounts and payouts, and to the complete history. The regulator or trust verifying agent receives compensation, whether a fee or as a percentage of the transaction amounts.

[0084] Next, the lotteries serve as the trusted agent, and receive a percentage of the transaction amount. Optionally, the historical functions of the lottery may be eliminated or vaporized from the system when those functions are performed by another entity within the ecosystem.

[0085] FIGS. **8** and **9** relate to the learning processes for training neural networks. By providing repeated input stimulus and then training the neural network to provide the correct output, the system may be taught to form the correct associated output based on one or more input stimuli. In converting input to the desired output the training may comprise supervised learning, such as when the target values and parameters are supervised. Alternatively, the training may be non-supervised learning, wherein the system attempts to identify patterns in the input that have identifiable structure and can be reproduced. Alternately, the system may use reinforcement learning, which works independently (like non-supervised learning) but is rewarded or punished depending on success or failure. Preferably, reinforcement learning involves incremental change. In the various training techniques, perturbation may be used wherein one or more input parameters are varied, typically in a perturbation amount, e.g., less than 10%, more preferably less than 5%, and most preferably less than 3%, of the input value, so as to monitor the effect of the perturbation on the output.

[0086] Hyperparameters and parameters may be used in the AI or machine learning systems. Model parameters are estimated from data automatically. A configuration variable internal to the model can be estimated from data. This can be required by the model when making predictions. Values define the skill of the model. They may be estimated or learned from data.

[0087] Hyperparameters are set manually and are used in the processes to help estimate parameters. A configuration variable external to the model is used. Generally, it cannot be estimated from the data. They are often used in processes to estimate model parameters. They are typically specified by the system user. Hyperparameters can often be set using heuristics. They are often tuned for a given predictive modeling problem. A hyperledger may be used, either as a hyperledger composer or hyperledger fabric.

[0088] The AI or machine learning may be performed on various types of hardware. Advantageously, systems that support parallel processing can provide for computation speed and efficiency. Parallel processing units such as Graphics Processing Units (GPUs) are available from NVIDIA and AMD. Neural Processing Units (NPUs) are available in the Kirin 970, Apple A11 and the Qualcomm Zeroth Processor. AI and machine learning processing is also available as a cloud AI or Machine learning system, such as is available from Google and Amazon Web Services.

[0089] FIG. **10** describes domain transformations and difference engines. One advantageous domain transformation involves the time domain to frequency domain (time series to frequency domain). One example is the Fourier series, which generally is used with repetitive signals, such as oscillating systems. A Fourier transform, is generally used with non-repetitive signals, such as transients. Enhanced computational techniques such as the Fast Fourier Transform (FFT) may be used for efficiency and computational speed. Yet another domain transformation is the Laplace transform, often used in electronic circuits and control systems. Yet another, the Z transform, is used with generally discrete-time signals. Digital Signal Processors (DSPs) may be advantageously utilized. Spectral density estimation may be included, along with wavelet analysis, image analysis, data compression and multivariate analysis. Correlated data sets are advantageously employed.

[0090] Difference engine may be employed to identify differences between two or more sets of data. The difference may be time based, such as where one data set relates to a time 0, and the other set relates to a time 1, time 2, time 3, . . . , time N. Differences in images may be calculated.

[0091] FIG. **11** shows a system in which the Subject response may be monitored, captured and analyzed for behavior, which is then used as input to AI. In various efforts, such as in game or entertainment design and creation, the response of the target audience may be monitored, analyzed and used to train an Artificial Intelligence or machine learning system. The subject response to entertainment/game stimuli serves to measure the 'fun' experienced by the subject, and that measure (the 'fun') is then used as a training input to AI or ML system. The system may detect individual subject behavior. Alternatively, the system may monitor group behavior, serving to detect the 'fun' experiences, but may also measure attributes of the group or crowd, such as 'excitement', 'engagement' or crowd based behavior.

[0092] A display is provided as a stimulus to the subject or subjects. A flat panel display or monitor may be utilized. Optionally, personal viewing devices may be utilized, such as individual screens, virtual reality headsets, augmented reality devices, heads up displays, projection devices or imaging technology.

[0093] Various detectors are utilized to monitor the one or more subject's response. Motion detection utilizes motion tracking hardware and software. A camera images the subjects. Various cameras include the Microsoft Kinect, 2d sensors and cameras and 3d sensors and cameras. Metrics detectors may analyze the position of a body part, such as a limb, joint or facial feature. It may measure the velocity, movement, higher level derivatives of the position or movement, such as the rate of change of change. Facial detectors monitor for facial recognition. Facial attributes may be detected, such as positive attributes, e.g., a smile, or negative attributes, e.g., a frown. Body position detection may be determined. Sound detection may be performed with a microphone or microphone array. It may detect attributes of the sound, such as positive attributes, e.g., a cheer, and negative attributes, e.g., expletives, and boos. Biometric scan detection is utilized. Physiologic response detection optionally monitors the subject heart rate, blood pressure, pupil dilation, temperature, ECG, and mental activity. Activity monitoring detectors monitor engagement response, preferably including bet rate, time spent engaged with the display, retention rate, repetition rate and reengagement rate. Analytics are advantageously utilized.

[0094] The output of the system is used as input in the AI or machine learning system. For example, in training using reinforcement learning in neural networks, a positive weighting is used for positive attributes, and a negative weighting is used for negative attributes.

[0095] The system may additionally provide output identified as associated with addiction, such as gambling addiction, or a subject otherwise being 'hooked' on the game. When the level of engagement or minor addiction is viewed as acceptable, a positive weighting may be used in the training, whereas when the addiction is viewed as unacceptable or excessive, a negative weighting may be used in the training.

[0096] The artificial intelligence, machine learning, neural network, use of user response in training AI/ML systems (generally FIG. **11** and discussion, above), may advantageously be utilized in game design and develop, entertainment development and/or any creative developmental effort.

[0097] The systems may constitute a matrix of tools. They may comprise a given set of tools. In a more fundamental way, they comprise a tool to discover the tools. Tools may be game states, entertainment states or any form of state or matter.

[0098] The following will be described as to game development, but the tools, systems, methods and architectures may be applied to entertainment or any creative effort. As to a particular game, a first option is to provide only basic rules of that given game. The system may play against itself, or alternatively, play against other systems, in order to discovery winning game play strategies. In yet another option, the system may be provided with known gambits, with the system permitted to use or ignore the gambits. In yet an alternative embodiment, the system may be provided with a library of games. The system may analyze the library of games for game elements, game mechanics or core loops. Optionally, the system may limit analysis of the library of games to similar games, or may consider all games, optionally divided into subunits, e.g. card games, board games, video games. Once the various core loops or game elements are defined, the system may combine them in various combinations and permutations so as to define a new game or game play sequence. The system may recognize patterns in the data. Values may be assigned to decisions at various points or game states or game state decision points. The use of user response may be advantageously used in game formation and optimization. The use of user response is particularly suited to reinforced learning.

[0099] The system may operate in a hierarchical manner. Hierarchical systems may be used, where it may vary a 'subservient' mandated parameter so long as 'superior' or 'master' mandated parameter is met. By way of example, a 'super' mandated parameter' may be used to guarantee a particular outcome. Alternatively, an administrative control may be granted, such as to set a 'top level' constraint.

[0100] The system may consider separate functions in a cooperative action. Functions may be reassigned or moved to other, especially lower, levels of action. The system may provide new variables. By providing a hierarchical response, core functionality may be maintained. Optionally, the system may employ a "kill switch" for the system, an apoptosis, such as based on a command such as from an administrator, or based on predefined criteria. The system may provide a package of experience ('Total Recall') such as in a continuous state and/or persistent state.

[0101] FIGS. **12** & **13** relate to various dynamic, that is changeable, systems. In the designation "d-API" and "d-SDK", 'd' stands for 'dynamic' and is capable of change within and by the system. The format of the interaction (request and/or response) may be changes. Alternately, it may change the type, quantity or quality of information provided in the response. Other factors that may be changed include the ability of the request to alter the information via the API or SDK. Changes may be made to other operational or administrative rights or permissions, such as read only access, read and write, edit rights, super administrative rights. These provide for dynamic change under adaptive control.

[0102] Within the dynamic-Application Programming Interface (d-API), an initial format for request and response is defined. This may be considered in an 'if-then' statement: IF you ask for X in an agreed upon format, THEN system will provide X. The dynamic system may vary the format, and/or response. An intelligent dynamic update may be based on AI, machine learning or analytics. While not limited to the following, some or all of these changes may be implemented dynamically: the format of the interaction (request and/or response), access to more information or functionality, e.g. read only, or modification rights, the ability to provide information or data to the system, and the ability to change data.

[0103] Within the dynamic Game Development Kit (d-GDK), an initial kit is provided. The system then permits dynamic modification of the GDK. Preferably, dynamic modification is based on AI or Machine Learning or analytics.

[0104] Dynamic Segregated Lottery (d-SL) may be provided wherein one or more functional units or the lottery may be provided. A virtualized system may be utilized, such as in the use of a virtualized server.

[0105] FIGS. **14-20** relate to a blockchain implementation for games, entertainment or other useful ends. Blockchain uses a cryptographic 'hash' to identifies each block and transaction. Each successive block contains a hash of the previous code. This permanently fixes transactions in chronological order. The blockchain utilizes both a private key and public key. The prior hash is added to the new blockchain with a nonce to form a new hash.

[0106] Cryptocurrency provides for cryptographically secure transactions. Cryptocurrency is a programmable currency or decentralized value transfer system. It is also a decentralized virtual currency or decentralized digital currency.

[0107] Proof of work, or proof of stake, is the "right" to participate in the blockchain. It must be onerous enough to prevent changes without redoing the work. Bitcoin is a created currency which is mined and serves as a reward for payment processing work. Blockchain cryptocurrency involves no transaction charges or fees paid by purchaser. There are no refund rights or chargebacks.

[0108] It may be implemented in any form of network, both public and private. Open software and proprietary software may be used. Storage may be local storage or cloud storage and computing. Analytics may be performed locally or in a cloud analytics system. Analytics As A Service (AAAS) may be performed. Systems may be permissioned v. permission less distributed systems.

[0109] FIGS. **21** through **23** relate to smart contracts. The core elements are, first, a set of promises which may be contractual or non-contractual. Second, they are specified in digital form, operate electronically, where the contractual clauses or functional outcomes embedded in code. Third, they include protocols, or technology enabled rules-based operations. Fourth, the parties perform on the promises through automated performance, in a generally irrevocable manner.

[0110] Smart contracts automate different processes and operations. In one embodiment, they automate "if-this-then-that" on self-executing basis with finality. They may provide for payments. Actions may be conditioned on a payment or payments, such as with the control of collateral based on payment.

[0111] Smart contracts may be implemented via blockchain. This forms a trusted system, which may be implemented in a business to business implementation (B to B) and/or peer-to-peer implementation. The machine-to-machine implementation permits various combinations. In one implementation, a blockchain is combined with devices comprising the Internet of Things (IoT). In yet another combination, the blockchain may be combined with devices comprising the Internet of Things in combination with artificial intelligence. Generally, the block contains smart contract program logic. It bundles together the messages relating to a particular smart contract including inputs, outputs, and logic. In yet another implementation, they may provide contracts for difference, such as in use the current market price to adjust balances and disperse cash flow.

[0112] Smart contracts are a trust shifting technology. They reduce counter-party risk. Preferably, this serves to increase credit.

[0113] Smart contracts may be implemented in various models. They may be a contract entirely in code. They may be a contract in code with separate natural language version. They may be split natural language contract with encoded performance. Alternatively, they may be a natural language contract with encoded payment mechanism.

[0114] Smart contract initiation involves a consensus. An algorithm constitutes a set of rules for how each participant in the contract processes messages. They may be implemented in a permission-less manner, wherein anyone may submit messages for processing. The submitter may be involved in consensus. Alternately, they may delegate decision making such as to an administrator or sub-group of participants. An alternative implementation is to have a permissioned system, in which the participants are limited. They are generally pre-selected. They are then subject to gated entry and be subject to the satisfaction of certain requirements and/or approval of an administrator.

[0115] Smart contracts are subject to various methods of formation. They may by agreement such as where there is a common cooperative opportunity or a defined desired outcome. These may include business practices, asset swaps, and transfer of rights. Next, conditions set for initiation of the contract. That may be by the parties themselves, or by the occurrence of some external event, such as time, other quantifiable measure or location. Typically, they generate a code, which is encrypted and chained with blockchain technology. It may be authenticated and verified. Upon execution and processing, the network updates all ledgers to indicate current state. Once verified and posted, they cannot be changed, with only additional blocks appended.

[0116] To restate, the smart contract serves as a distributed application on networks with independent built-in trust mechanisms. The program is entrusted with the unit of value combined with rules for transfer of ownership of the unit of value. They serve as self-executing programs that automatically fulfill the terms of a programmed relationship.

[0117] FIG. **20** shows a Lottery embodiment implemented as a smart contract. The method for implementing a lottery includes the following steps. A time frame is set in which to receive cryptocurrency. Second, cryptocurrency is received with owner identification within the timeframe. The window opens for a specified duration, afterwards at which the window closes. The smart contract generates or receives a random event, such as from a random number generator. The random number generator should include an algorithmic guarantee of randomness and a guarantee of no hack. The contract selects a new owner (winner) among the owner identification related cryptocurrencies. It then assigns new ownership of cryptocurrency to selected new owner (winner).

[0118] Smart contracts may be used to implement a core loop or a game mechanic. The following core loops and game mechanics comprise a partial list of those that may be implemented, including but not limited to JACKO, POKO, Hot Seat, Hi Lo, Rock, Paper Scissors, In the Zone and iLotto or other array or geography based game mechanics or core loops. Any subunit of the game mechanic or core loop may itself be used as a game mechanic or core loop.

[0119] Jacko is a game comprising the steps of: randomly selecting a target number from a first range of numbers having a minimum and maximum number, presenting an indication of the target number to the player, selecting a number for the player, the number being selected from a second range, having a minimum and maximum, where the maximum is equal to or less than 52 of the minimum of the first range, receiving an indication from the player whether to draw again, and if so, randomly selecting a number from the second range, accumulating the total of the player's draws, and repeating this step until either the player declines to draw or the total exceeds the target number, and in the event the player declines to draw, randomly selecting numbers from the second range, accumulating those numbers, comparing them to the player's accumulated amount, and assigning as to the winner whomever has a total closest to, but not exceeding, the target.

[0120] Poko is a multi-player game where multiple indicia are awarded a predefined value, where other players have no information as to at least some of the indicia held by other players.

[0121] High Lo is a game comprising the steps of: performing a first lottery selection of a series of randomly drawn numbers, receiving from a player an indication whether the next randomly drawn number will be higher or lower than the preceding number, and if correct, awarding winnings correlated to the amount of the randomly drawn number, and continuing until the player fails to predict the high/low outcome, or elects to stop.

[0122] In the Zone is a game of chance comprising the steps of randomly selecting a player's target number within a predefined range of numbers, the range having a minimum and a maximum, randomly selecting a series of numbers for use in a lottery game, the minimum of the predefined range of numbers being at least equal to the sum of the lowest possible total for the series of the lowest possible total for the series of numbers and the maximum of the predefined range of numbers, totaling the random selected series of numbers through the conclusion of the selection, and assigning prize amounts to players having a player's number not exceeding the total based upon the proximity of the player's number and the total number.

[0123] Rock Paper Scissors is a game with three or more options having an assigned priority of options relative to one another.

[0124] Hot Seat is a game of increasing risk/reward including the ability to 'opt out' in Smart Contract. A method for game play in a multi-level game of chance culminating in a final level, comprises the steps of presenting, at a given level, a plurality of random options wherein at least one option is a positive option, another option is a negative option, and a third option requiring a further decision, receiving a selection regarding which one of the plurality of random option is selected, and if the positive option was selected, cumulating the positive option result with the prior positive option results, but if the negative option was selected, cumulating the negative option result, comparing the cumulative result with a predetermined number, and replaying the same level if the cumulative number is less than the predetermined number or terminating the game if the cumulative number equals the predetermined number, and if the third option was selected, receiving a selection regarding the decision, respecting the above steps until the player stops, the predetermined number of negative events occurring or the final level is related.

[0125] iLotto is a grid or geography based system including a display for presenting a grid of identifying objects, an input for receiving a player selection of an identifying object, a random generator for randomly selecting a winning identifying object, and a point tally system for awarding points to the player according to the rules comprising a first point value if the player selected identifying object exactly matches the winning identifying object, a second point value if the player selected identifying object is in a geometric relationship with the winning identifying object, and a third, negative, point value if the player is not awarded the first point value or the second point value.

[0126] FIG. **23** relates to implementation of mandated and variable parameters. Mandated parameters are set in smart contracts. Examples of mandated parameters include payout percentage and payout amount. Variable parameters are subject to mandated parameters, providing entertainment options.

[0127] FIG. **24** depicts a wallet serving for the electronic storage of cryptocurrency. This represents a graphical user interface ("GUI"), such as on a phone or computer display. Various forms of cryptocurrency may be displayed on the GUI and stored in the wallet. Points may be awarded, such as for loyalty, frequency and airtimes. Recent or latest transactions may be listed, indicating the date, purpose and amount. A total account value may be shown.

[0128] Cryptocurrency systems and smart contracts may be implemented in combination with other systems. One additional system comprises a frequent user or player's club system. They may be combined with other forms of 'currency lite', including micro-transactions and micro-payments. They may be used in combinations with smart properties, that is digital assets or physical things that know who their owner is. Digital assets are anything that exists in digital, typically binary, format and comes with the right to use. Examples include images, including still pictures and video or dynamic images, audible content, such as sounds, music or performances, and digital documents. Property whose ownership is controlled via distributed trusted network, e.g., blockchain using contracts. They may be further used in combination with geolocation, wherein the physical location (geolocation) of various components and architectural components are optionally a component of the system. Limits may be placed on the geography of game play. The system can ensure compliance with geolocation of data routing.

[0129] FIGS. **25** through **27** relate to systems having segregated secure functions and public functions. This provides a secure platform with multiple interfaces to public functions and public entities. The segregated secure functions provide the function of the trusted agent. The secure functions include one or more of the following. First, outcome determination. This may include the use of a random number generator (RNG) or probability engine. Second, user or player account information is stored. Third, monetary accounting or transactions are stored. Fourth, regulatory and compliance interface is performed. Fifth, interfaces such as a developer interface. Sixth, regulatory functions including Q&A testing, compliance, testing and approval may be provided.

[0130] The public functions include some or all of the following. First, the public system issues a 'call' to the secure system. A 'call' may be via an Application Programming Interface (API) or d-API. The "OPEN" system call makes calls to secure system for secure data. Second, a designer interface serves to access tools, APIs, a Development Kit (DK), and a Software Development Kit (SDK). Third, a marketplace interface serves as a lottery interface and optionally an application or app store. Fourth, an operator interface serves to interface with an operator or organizer, e.g., a charity. It preferably serves to publish, market, and sell. Fifth, the user interface permits registration, play activity and persistent history.

[0131] The system components may vary by function. Public interfaces and functions preferably comprise an "open" platform. This allows for arbitration and agreement with the secure entity regarding game operations to be performed by the secure entity, e.g., payout %, vGLEPs, who may play, and geolocation. The secure entity performs secure functions including game outcomes, financial matters and secure user data. The end users utilize a "channel mix", including but not limited to web, mobile app, mobile web, tablet, computer, display enabled Devices (wireless), touch screen equipment at retailer, e.g., countertop games. The private entity may impose rate limits and impose responsible gaming controls.

[0132] FIGS. **28** and **29** describe hybrid and hierarchical systems. A centralized system, such as a state run lottery may be combined with a decentralized system, such as a blockchain implementation. Hierarchical order may be imposed within the system. In a system using mandated and variable parameters, a hierarchy of mandated parameters may be established, and then various variable parameters may be subject to the appropriate mandated parameter. In another application, a global use rate limit may be imposed at a high level in the hierarchy. Hierarchical use rate limits may be imposed. Various topologies of systems include master slave, master over multiple slaves and circular systems.

[0133] FIG. **30** relates to a game or lottery linked credit card and credit card function. A credit card and credit functionality may be linked to lottery or other game play. Through use of the credit card, a conversion rate is established. By way of example, for every $100 of purchases, $ 1 in lottery play is made. The rate may be variable, such as based upon institution. In the event a charitable organization organized or sponsored the lottery or game, every $100 of purchases accrues $2 for the organization. A split may also be performed, such as for every $100 of purchases accrues $1 in the lottery or game for the credit card owner and $1 for the organization.

[0134] In alternative embodiments, the mobile gaming device may be connected to the gaming machine with a cable, either directly connected to a port of the gaming machine or via a network communicating with the gaming machine.

[0135] The software used to program the gaming machines and servers in accordance with the embodiments described herein may be initially stored on a ROM, such as a CD or an electronic memory device. Such CDs and devices are non-transitory computer readable mediums having the appropriate computer instructions stored thereon. The programming may also be downloaded to the gaming machines via the casino's network.

[0136] It should be appreciated that the terminals, processors, or computers described herein may be embodied in any of a number of forms, such as a rack-mounted computer, a desktop computer, a laptop computer, or a tablet computer. Additionally, a computer may be embedded in a device perhaps not generally regarded as a computer but with suitable processing capabilities, including an electronic gaming machine, a Web TV, a Personal Digital Assistant (PDA), a smart phone or any other suitable portable or fixed electronic devices.

[0137] Also, a computer may have one or more input and output devices. These devices can be used, among other things, to present a user interface. Examples of output devices that can be used to provide a user interface include printers or display screens for visual presentation of output and speakers or other sound generating devices for audible presentation of output. Examples of input devices that can be used for a user interface include keyboards, and pointing devices, such as mice, touch pads, and digitizing tablets. As another example, a computer may receive input information through speech recognition or in other audible formats.

[0138] Such computers may be interconnected by one or more networks in any suitable form, including as a local area network or a wide area network, such as an enterprise network or the Internet. Such networks may be based on any suitable technology and may operate according to any suitable protocol and may include wireless networks, wired networks or fiber optic networks. As used herein, the term "online" refers to such networked systems, including computers networked using, e.g., dedicated lines, telephone lines, cable or ISDN lines as well as wireless transmissions. Online systems include remote computers using. e.g., a local area network (LAN), a wide area network (WAN), the Internet, as well as various combinations of the foregoing. Suitable user devices may connect to a network for instance, any computing device that is capable of communicating over a network, such as a desktop, laptop or notebook computer, a mobile station or terminal, an entertainment appliance, a set-top box in communication with a display device, a wireless device such as a phone or smartphone, a game console, etc. The term "online gaming" refers to those systems and methods that make use of such a network to allow a game player to make use of and engage in gaming activity through networked, or online systems, both remote and local. For instance. "online gaming" includes gaming activity that is made available through a website on the Internet.

[0139] Also, the various methods or processes outlined herein may be coded as software that is executable on one or more processors that employ any one of a variety of operating systems or platforms. Additionally, such software may be written using any of a number of suitable programming languages and/or programming or scripting tools, and also may be compiled as executable machine language code or intermediate code that is executed on a framework or virtual machine.

[0140] In this respect, embodiments may provide a tangible, non-transitory computer readable storage medium (or multiple computer readable storage media) (e.g., a computer memory, one or more floppy discs, compact discs (CD), optical discs, digital video disks (DVD), magnetic tapes, flash memories, circuit configurations in Field Programmable Gate Arrays or other semiconductor devices, or other non-transitory, tangible computer-readable storage media) encoded with one or more programs that, when executed on one or more computers or other processors, perform methods that implement the various embodiments discussed above. The computer readable medium or media can be transportable, such that the program or programs stored thereon can be loaded onto one or more different computers or other processors to implement various aspects as discussed above. As used herein, the term "non-transitory computer-readable storage medium" encompasses only a computer-readable medium that can be considered to be an article of manufacture or a machine and excludes transitory signals.

[0141] The terms "program" or "software" are used herein in a generic sense to refer to any type of computer code or set of computer-executable instructions that can be employed to program a computer or other processor to implement various aspects of, as discussed above. Additionally, it should be appreciated that according to one aspect of this embodiment, one or more computer programs that when executed perform methods need not reside on a single computer or processor, but may be distributed in a modular fashion amongst a number of different computers or processors to implement various aspects of embodiments described herein.

[0142] Computer-executable instructions may be in many forms, such as program modules, executed by one or more computers or other devices. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Typically the functionality of the program modules may be combined or distributed as desired in various embodiments.

[0143] Also, data structures may be stored in computer-readable media in any suitable form. For simplicity of illustration, data structures may be shown to have fields that are related through location in the data structure. Such relationships may likewise be achieved by assigning storage for the fields with locations in a computer-readable medium that conveys relationship between the fields. However, any suitable mechanism may be used to establish a relationship between information in fields of a data structure, including through the use of pointers, tags, addresses or other mechanisms that establish relationship between data elements.

[0144] Various aspects of embodiments described herein may be used alone, in combination, or in a variety of arrangements not specifically discussed in the embodiments described in the foregoing and the concepts described herein are therefore not limited in their application to the details and arrangement of components set forth in the foregoing description or illustrated in the drawings. For example, aspects described in one embodiment may be combined in any manner with aspects described in other embodiments.

[0145] Also, embodiments described herein may provide a method, of which an example has been provided. The acts performed as part of the method may be ordered in any suitable way. Accordingly, embodiments may be constructed in which acts are performed in an order different than illustrated, which may include performing some acts simultaneously, even though shown as sequential acts in illustrative embodiments.

[0146] While embodiments have been described with reference to certain exemplary features thereof, those skilled in the art may make various modifications to the described embodiments. The terms and descriptions used herein are set forth by way of illustration only and not meant as limitations. In particular, although embodiments have been described by way of examples, a variety of devices would practice the inventive concepts described herein. Embodiments have been described and disclosed in various terms, the scope of the embodiments is not intended to be, nor should it be deemed to be, limited thereby and such other modifications or embodiments as may be suggested by the teachings herein are particularly reserved, especially as they fall within the breadth and scope of the claims here appended. Those skilled in the art will recognize that these and other variations are possible as defined in the following claims and their equivalents. Although the foregoing invention has been described in some detail by way of illustration and example for purposes of clarity and understanding, it may be readily apparent to those of ordinary skill in the art in light of the teachings of this invention that certain changes and modifications may be made thereto without departing from the spirit or scope of the appended claims.

[0147] All publications and patents cited in this specification are herein incorporated by reference as if each individual publication or patent were specifically and individually indicated to be incorporated by reference in their entirety.

REFERENCES

[0148] ARM, IBM, "The Internet of Things Business Index 2017, Transformation In Motion", The Economist, Intelligence Unit Limited 2017, pages 1-22.

[0149] Crosby, et al., "Blockchain Technology: Beyond Bitcoin", Applied Innovation Review, Issue No. 2, Sutardja Center for Entrepreneurship & Technology, Berkeley Engineering, June 2016, pages 1-19.

[0150] Fisher, "Decentralized Peer to Peer Game Assets Platform, Integration with Third Party Games using Smart Contract," Aug. 4, 2014, 12 pages.

[0151] Hinton et al., "A Fast Learning Algorithm For Deep Belief Nets". Neural Computation, 18, 1527-1554, 2006.

[0152] Jouppi, et al., "In-Datacenter Performance Analysis of a Tensor Processing Unit™", To appear at the 44th International Symposium on Computer Architecture (ISCA), Toronto, Canada, Jun. 26, 2017, pages 1-17.

[0153] LeCun, et al., "Deep Learning", Nature, Vol. 521, 28 May 2015, pages 436-444.

[0154] Marvin, "Blockchain A-Z: Everything You Need to Know About the Game-Changing Tech Beneath Bitcoin". Jun. 3, 2016, 9 pages.

[0155] Marvin, "Blockchain: The Invisible Technology That's Changing the World", Feb. 6, 2017, 32 pages.

[0156] Mougayar, The Business Blockchain, pages 6-9, 128-133, 2016, published by John Wiley & Sons, Hoboken, N.J.

[0157] Nakamoto, "Bitcoin—A Peer to Peer Electronic Cash System", 2008, pages. 1-9

[0158] Ng, "What Artificial Intelligence Can and Can't Do Right Now", Harvard Business Review, Nov. 9, 2016, 5 pages.

[0159] O'Dowd, et al., "IBM's Open Blockchain, Making Blockchain Real for Enterprises", IBM Blockchain, April 2016, pages 1-20.

[0160] Ronan, "Deep Learning predicts Loto Numbers", Academy of Paris, Apr. 1, 2016, pages 1-4.

[0161] Smart Contract Alliance, "Smart Contracts: 12 Use Cases for Business and Beyond, A Technology, Legal & Regulatory Information, prepared by Smart Contracts Alliance—In collaboration with Deloitte, An industry initiative of the Chamber of Digital Commerce". December 2016, pages 1-53.

[0162] Turing, "Computing Machinery and Intelligence", Mind 49: 1950, pages 433-460.

[0163] Wood, "Ethereum: A Secure Decentralized Generalized Transaction Ledger", Homestead Draft, 2014, pages 1-32.

[0164] Wu, et al., "Google's Neural Machine Translation System: Bridging the Gap between Human and Machine Translation", 8 Oct. 2016, pages 1-23.

[0165] Yli-Huumo, et al., "Where Is Current Research on Blockchain Technology? A Systematic Review", Oct. 3, 2016, pages 1-27.

Glossary

[0166] 51% Attack: An attack on the Bitcoin network which allows the attacker to create fraudulent transactions, see Double Spend. This is possible because controlling more than 50% of the Bitcoin network's hash rate means the attacker can out-compute everyone else who is mining.

A

[0167] Account: Accounts have an intrinsic balance and transaction count maintained as part of the Ethereum state. They also have some (possibly empty) EVM Code and a (possibly empty) Storage State associated with them. Though homogenous, it makes sense to distinguish between two practical types of account: those with empty associated EVM Code (thus the account balance is controlled, if at all, by some external entity) and those with non-empty associated EVM Code (thus the account represents an Autonomous Object). Each Account has a single Address that identifies it.

[0168] Address: A bitcoin address is used to receive and send transactions on the bitcoin network. It contains a string of alphanumeric characters, but can also be represented as a scannable QR code. A bitcoin address is also the public key in the pair of keys used by bitcoin holders to digitally sign transactions (see Public Key).

[0169] Address: A code, e.g. a 160-bit code, used for identifying Accounts.

[0170] Agreement Ledger: An agreement ledger is distributed ledger used by two or more parties to negotiate and reach agreement.

[0171] Airdrop: A method of distributing cryptocurrency amongst a population, first attempted with Auroracoin (auroracoin) in early 2014.

[0172] Algorithm: A process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer.

[0173] Altcoin: The collective name for cryptocurrencies offered as alternatives to bitcoin. Litecoin, Feathercoin and PPcoin are all altcoins.

[0174] AML: Anti-Money Laundering techniques are used to stop people converting illegally obtained funds, to appear as though they have been earned legally. AML mechanisms can be legal or technical in nature. Regulators frequently apply AML techniques to bitcoin exchanges.

[0175] App: An end-user-visible application, e.g. hosted in the Ethereum Browser.

[0176] Application Program Interface (API): A specification used as an interface by components, often software components, to communicate with one another. May include specifications for routines, data structures, object classes, and variables.

[0177] Arbitrage: The generation of risk free profits by trading between markets which have different prices for the same asset.

[0178] ASIC: An Application Specific Integrated Circuit is a silicon chip specifically designed to do a single task. In the case of bitcoin, they are designed to process SHA-256 hashing problems to mine new bitcoins.

[0179] ASIC Miner: A piece of equipment containing an ASIC chip, configured to mine for bitcoins. They can come in the form of boards that plug into a backplane, devices with a USB connector, or standalone devices including all of the necessary software, that connect to a network via a wireless link or ethernet cable.

[0180] ASIC Mining: Many miners purchase separate computing devices set aside solely for mining. As an alternative, they can also get an Application Specific Integrated Circuit (ASIC); this is a specially-designed computer chip created to perform one specific function, and only that function—in this case, mining calculations. ASICs reduce the processing power and energy required for mining, and can help reduce the overall cost of the process in that way. Whether the ASIC—a term that refers to the specialized chip itself—is integrated into an existing computing system, or functions as a stand-alone device, the term "ASIC" is often used generically to refer to the overall system itself, and not just the chip.

[0181] Asymmetric Key Algorithm: This is the algorithm used to generate public and private keys, the unique codes that are essential to cryptocurrency transactions. In a symmetric key algorithm, both the sender and receiver have the same key; they can encrypt and exchange information privately, but since both parties have the decoding information, they can't keep information private from one another. With an asymmetric key algorithm, both parties have access to the public key, but only the person with the private key can decode the encryption; this assures that only they can receive the funds.

[0182] Attestation Ledger: A distributed ledger providing a durable record of agreements, commitments or statements, providing evidence (attestation) that these agreements, commitments or statements were made.

[0183] Autonomous Agents: Software that makes decisions and acts on them without human intervention.

[0184] Autonomous Object: A notional object existent only within the hypothetical state of Ethereum. Has an intrinsic address and thus an associated account; the account will have non-empty associated EVM Code. Incorporated only as the Storage State of that account.

B

[0185] Base58: Base58 encodes binary data into text and is used to encode Bitcoin addresses. Created by Satoshi Nakamoto, its alphanumeric characters exclude "0", "O", "1", I" since they are hard to distinguish.

[0186] Base58Check: A variant of Base58 used to detect typing errors in bitcoin addresses.

[0187] BIP: An acronym for "Bitcoin Improvement Proposals" which can be submitted by anyone who wants to improve the Bitcoin network.

[0188] Bit: Name of a Bitcoin denomination equal to 100 satoshis (1 millionth of 1 BTC). In 2014 several companies including Bitpay and Coinbase, and various wallet apps adopted bit to display bitcoin amounts.

[0189] Bitcoin (uppercase): The well know cryptocurrency, based on the proof-of-work blockchain.

[0190] bitcoin (lowercase): The specific collection of technologies used by Bitcoin's ledger, a particular solution. Note that the currency is itself one of these technologies, as it provides the miners with the incentive to mine.

[0191] Bitcoin (unit of currency): 100,000,000 satoshis. A unit of the decentralized, digital currency which can be traded for goods and services. Bitcoin also functions as a reserve currency for the altcoin ecosystem.

[0192] Bitcoin 2.0: A reference word for applications of bitcoin or Blockchain technology that is more advanced or complicated than the basic payment system application proposed by the Bitcoin white paper. Examples of Bitcoin 2.0 projects include Counterparty, Ethereum, Blockstream, Swarm, Domus and Hedgy.

[0193] Bitcoin ATM: A bitcoin ATM is a physical machine that allows a customer to buy bitcoin with cash. There are many manufacturers, some of which enable users to sell bitcoin for cash. They are also sometimes called 'BTMs' or 'Bitcoin AVMS'. CoinDesk maintains a worldwide map of operational bitcoin ATM machines and a list of manufacturers.

[0194] Bitcoin Core: New name of Bitcoin QT since release of version 0.9 on Mar. 19, 2014. Not to confuse with CoreBitcoin, an Objective-C implementation published in August 2013.

[0195] Bitcoind: Original implementation of Bitcoin with a command line interface. Currently a part of BitcoinQT project. "D" stands for "daemon" per UNIX tradition to name processes running in background.

[0196] Bitcoin Days Destroyed: An estimate for the "velocity of money" with the Bitcoin network. This is used because it gives greater weight to bitcoins that have not been spent for a long time, and better represents the level of economic activity taking place with bitcoin than total transaction volume per day.

[0197] Bitcoin Investment Trust: This private, open-ended trust invests exclusively in bitcoins and uses a state-of-the-art protocol to store them safely on behalf of its shareholders. It provides a way for people to invest in bitcoin without having to purchase and safely store the digital currency themselves.

[0198] Bitcoinj: A Java implementation of a full Bitcoin node by Mike Hearn. Also includes SPV implementation among other features.

[0199] BitcoinJS: An online library of javascript code used for Bitcoin development, particularly web wallets. bitcoinjs.org(http://bitcoinjs.org)

[0200] Bitcoin Market Potential Index (BMPI): The Bitcoin Market Potential Index (BMPI) uses a data set to rank the potential utility of bitcoin across **177** countries. It attempts to show which markets have the greatest potential for bitcoin adoption.

[0201] Bitcoin Network: The decentralized, peer-to-peer network which maintains the blockchain. This is what processes all Bitcoin transactions.

[0202] Bitcoin Price Index (BPI): The CoinDesk Bitcoin Price Index represents an average of bitcoin prices across leading global exchanges that meet criteria specified by the BPI. There is also an API for developers to use.

We claim:

1. A system for control of an entertainment state system having segregated secure functions and public functions for use by one or more users of the system, comprising:

a public interface portal, the interface portal adapted to receive instructions regarding operation of the entertainment state system from the one or more users, the interface portal including:

a first interface to receive instructions from and communicate to the one or more end users,

a processor,

a graphical user interface (GUI) coupled to the processor,

a control unit in operative communication with the processor and graphical user interface, and

a second interface providing an application program interface (API), and

a secure entity unit, the secure entity unit including:

a receive interface, the receive interface adapted to receive a call from the application program interface (API) of the interface portal,

a send interface, the send interface adapted to provide a response to the interface portal interface,

a game engine,

a financial engine, the financial engine being coupled to the game engine, and the receive interface and send interface,

and an interface to provide financial information.

2. The system for the control of an entertainment state system of claim **1** wherein the secure entity further includes memory to store user secure information.

3. The system for the control of an entertainment state system of claim **1** wherein the financial information is tax information.

4. The system for the control of an entertainment state system of claim **1** wherein the financial information couples to a financial institution.

5. The system for the control of an entertainment state system of claim **1** wherein the game engine includes a game random number generator (RN).

6. The system for the control of an entertainment state system of claim **1** wherein the secure entity further includes an adaptive control unit.

7. The system for the control of an entertainment state system of claim **6** wherein the adaptive control unit includes cognitive computing unit.

8. The system for control of an entertainment state system of claim **6** wherein the adaptive control unit includes an artificial intelligence unit.

9. The system for control of an entertainment state system of claim **1** wherein the adaptive control unit includes a machine-learning unit.

10. The system for control of an entertainment state system of claim **1** wherein the adaptive control unit includes a neural network.

11. The system for control of an entertainment state system of claim **10** wherein the neural network is a deep neural network.

12. The system for control of an entertainment state system of claim **10** wherein the neural network includes a graphics processing unit (GPU).

13. The system for control of an entertainment state system of claim **10** wherein the neural network is trained utilizing user response data.

14. The system for control of an entertainment state system of claim **10** wherein the neural network is a vectorized neural network.

15. The system for control of an entertainment state system of claim **10** wherein the neural network is a recurrent neural network.

16. The system for control of an entertainment state system of claim **1** wherein the secure entity includes an analytics unit.

* * * * *

US 20180247191A1

(19) **United States**

(12) **Patent Application Publication**

(10) **Pub. No.: US 2018/0247191 A1**

Katz et al.

(43) **Pub. Date: Aug. 30, 2018**

(54) **ARCHITECTURES, SYSTEMS AND METHODS FOR PROGRAM DEFINED ENTERTAINMENT STATE SYSTEM, DECENTRALIZED CRYPTOCURRENCY SYSTEM AND SYSTEM WITH SEGREGATED SECURE FUNCTIONS AND PUBLIC FUNCTIONS**

(71) Applicant: **MILESTONE ENTERTAINMENT LLC**, Beverly Hills, CA (US)

(72) Inventors: **Randall M. Katz**, Beverly Hills, CA (US); **Robert Tercek**, Hollywood, CA (US)

(21) Appl. No.: **15/886,432**

(22) Filed: **Feb. 1, 2018**

Related U.S. Application Data

(60) Provisional application No. 62/454,423, filed on Feb. 3, 2017.

Publication Classification

(51) **Int. Cl.**

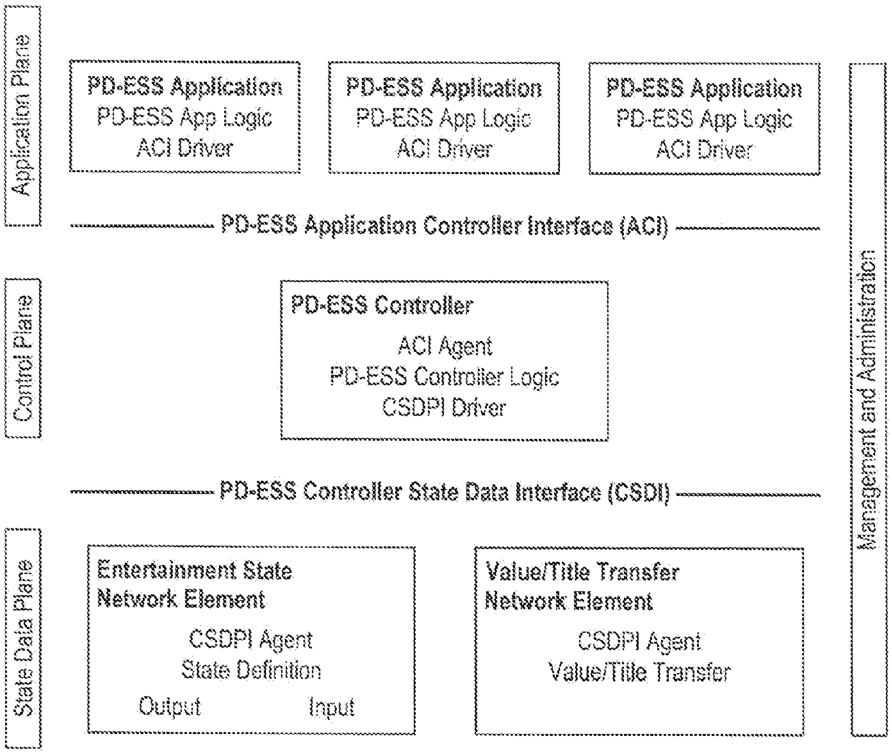
G06N 3/08	(2006.01)
G06K 9/00	(2006.01)
G06Q 20/06	(2006.01)
G07F 17/32	(2006.01)

(52) **U.S. Cl.**

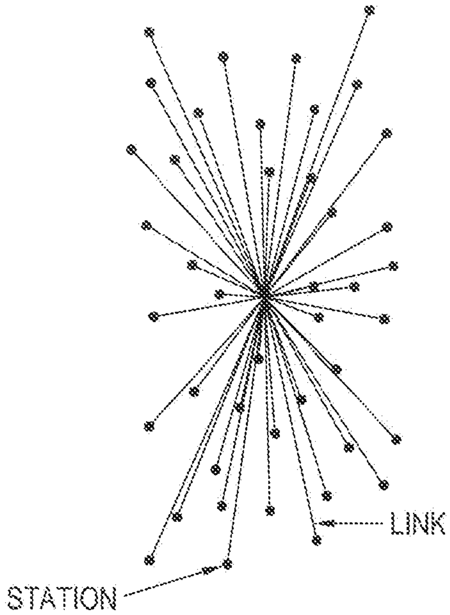
CPC ***G06N 3/08*** (2013.01); ***G07F 17/329*** (2013.01); ***G06Q 20/065*** (2013.01); ***G06K 9/00221*** (2013.01)

(57) **ABSTRACT**

Systems and methods are provided for training an artificial intelligence system including the use of one or more human subject responses to stimuli as input to the artificial intelligence system. Displays are oriented to the human subjects to present the stimuli to the human subjects. Detectors monitor the reaction of the human subjects to the stimuli, the detectors including at least motion detectors, the detectors providing an output. An analysis system is coupled to receive the output of the detectors, the analysis system provides an output corresponding to whether the reaction of the human subjects was positive or negative. A neural network utilizes the output of the analysis system, generating a positive weighting for training of the neural network when the output of the analysis system was positive, and a negative weighting for training of the neural network when the output of the analysis system was negative.



Programmatically Defined Gaming System

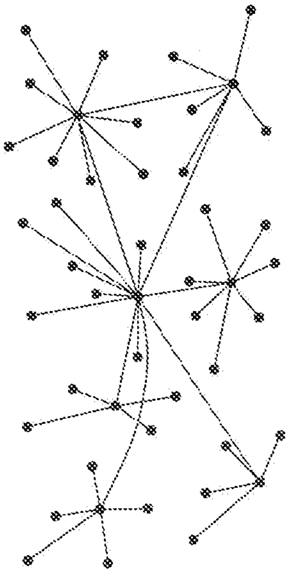


CENTRALIZED (A)

Prior Art Centralized System

FIG. 1

(Prior Art)

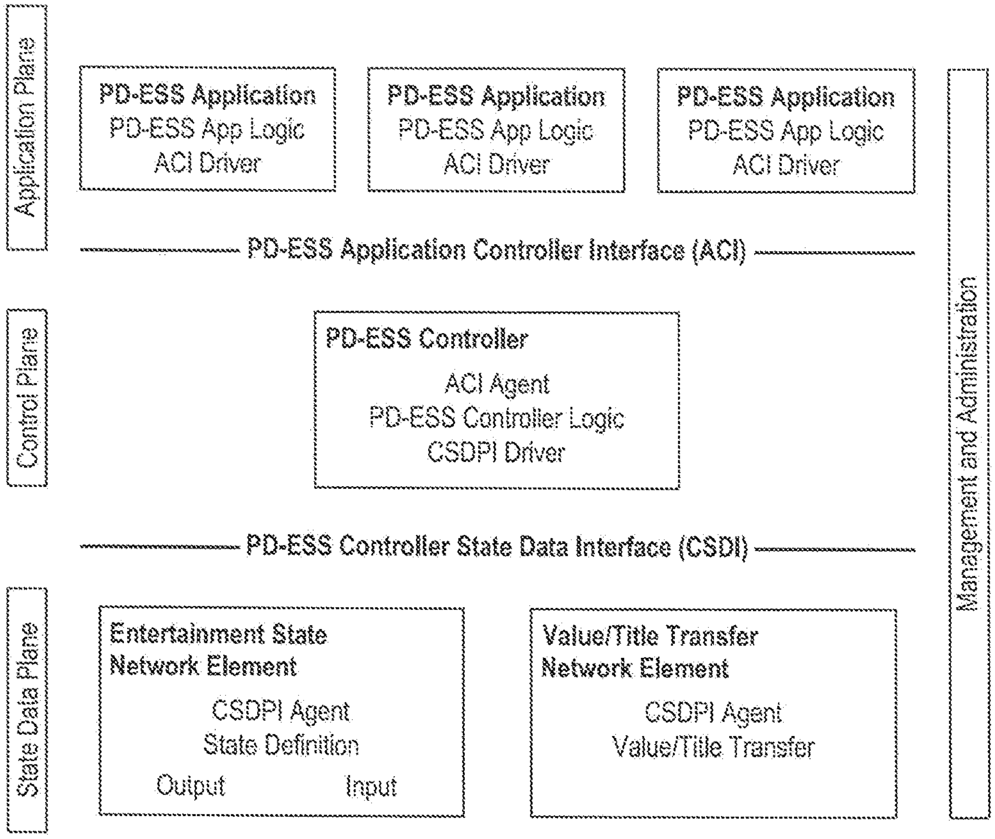


DECENTRALIZED

Prior Art Decentralized System

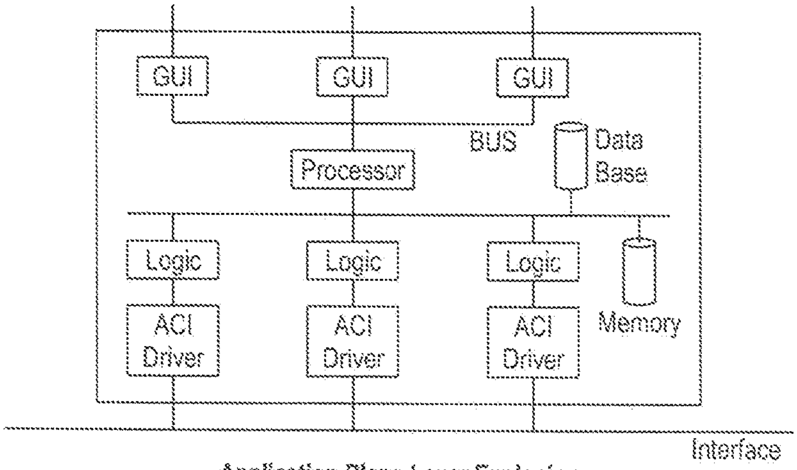
FIG. 2

(Prior Art)



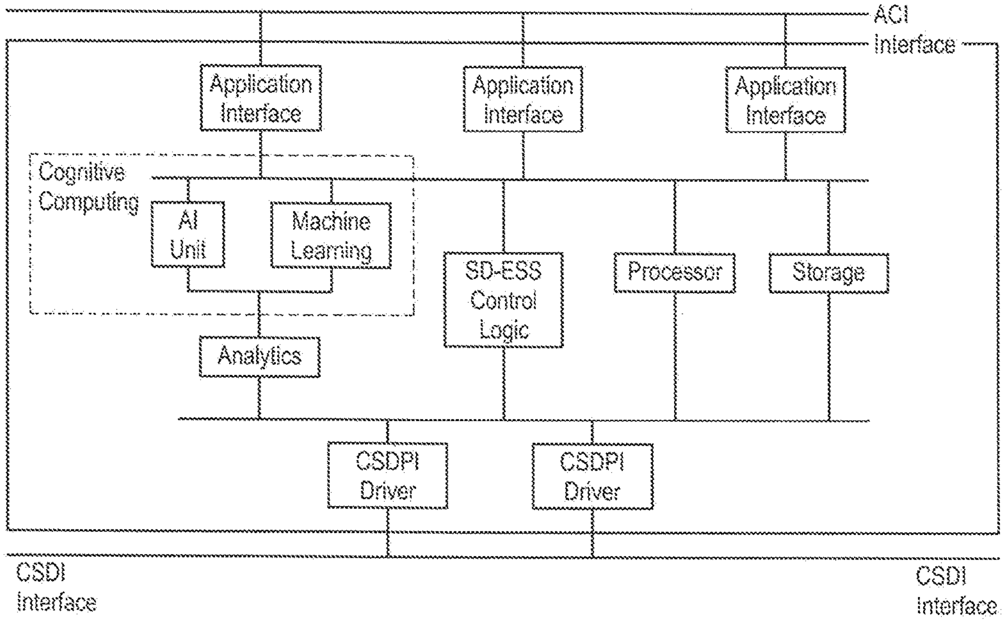
Programmatically Defined Gaming System

FIG. 3



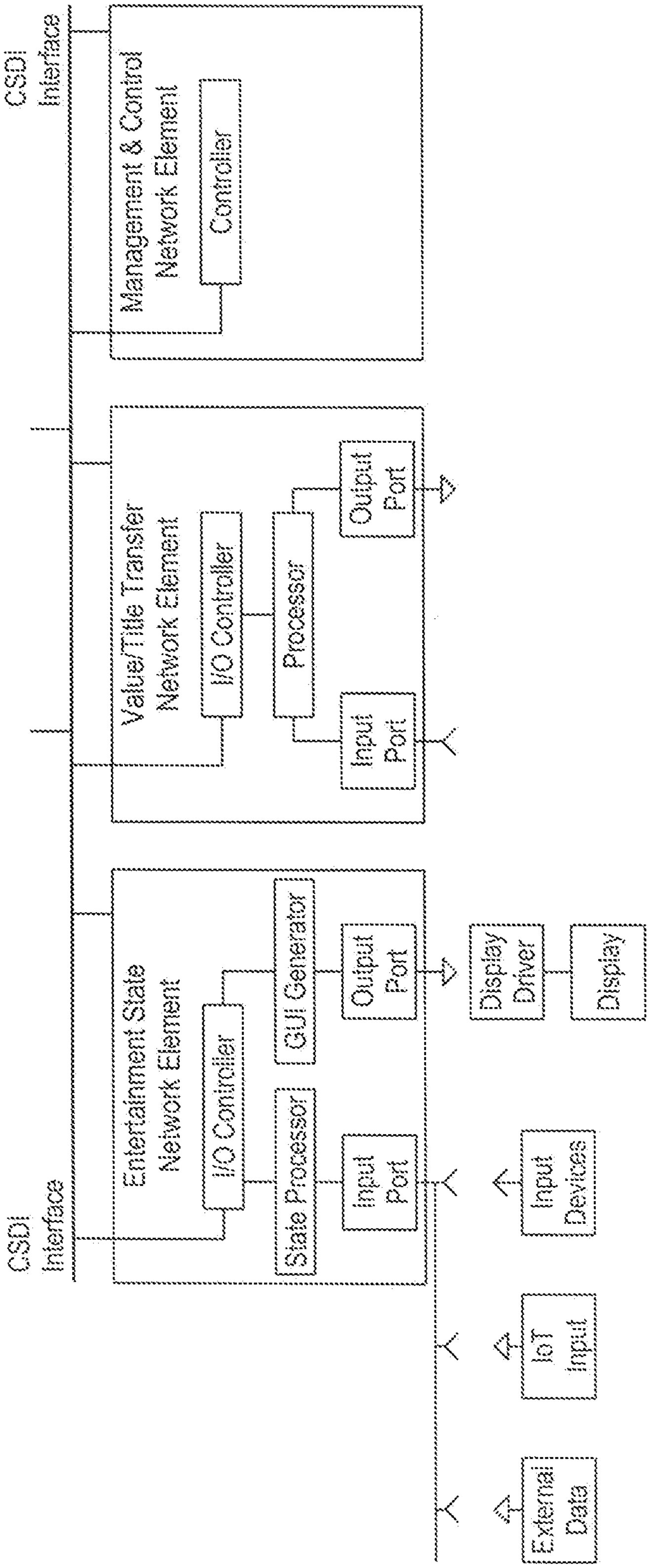
Application Plane Layer Explosion

FIG. 4



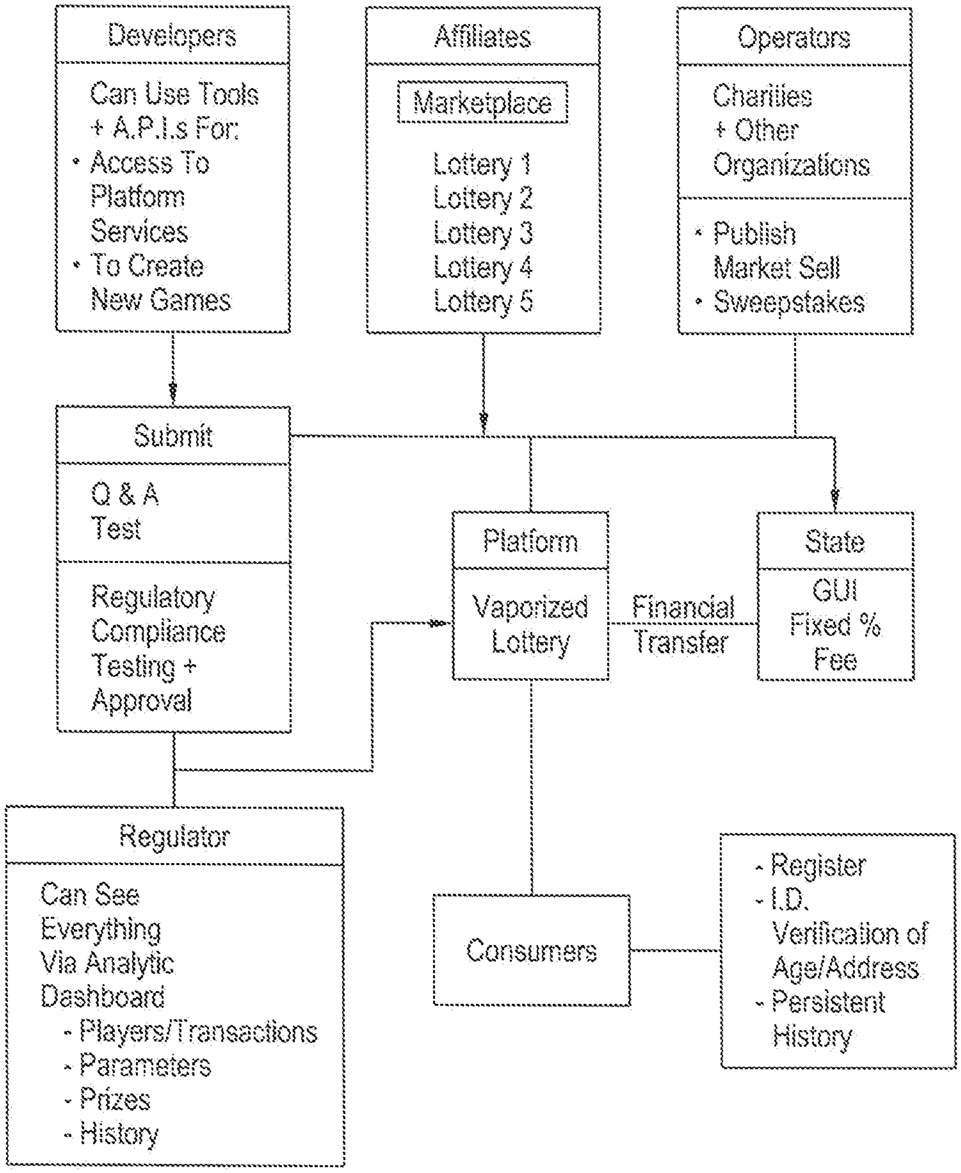
Control Plane Layer Explosion

FIG. 5



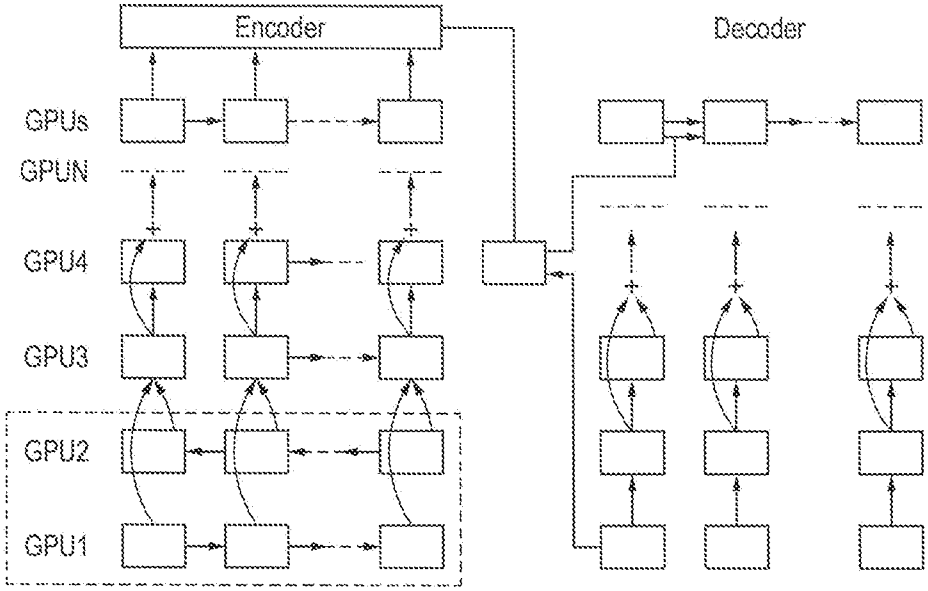
State Data Plane Layer Explosion

FIG. 6



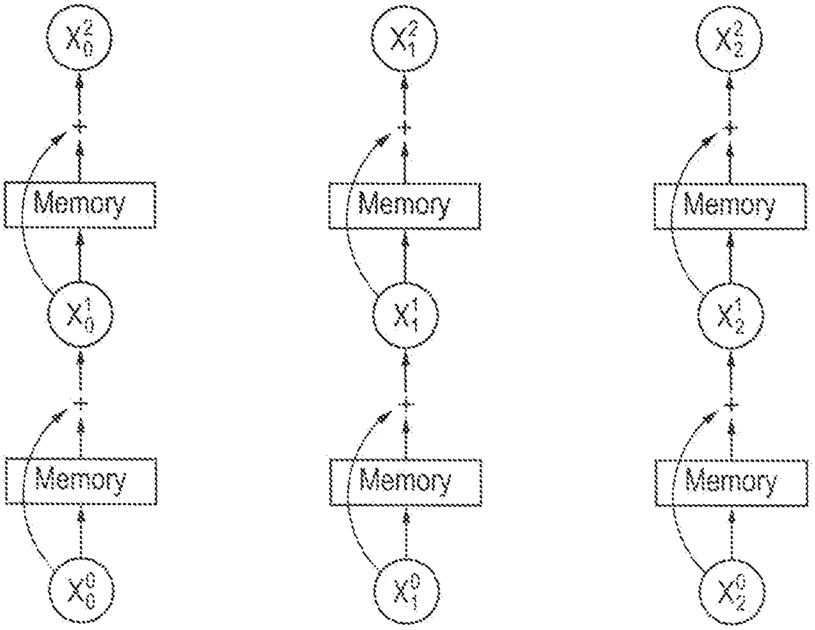
Ecosystem Interfaces and Interconnections

FIG. 7



Neural Network Model Architecture

FIG. 8



Neural Network

FIG. 9

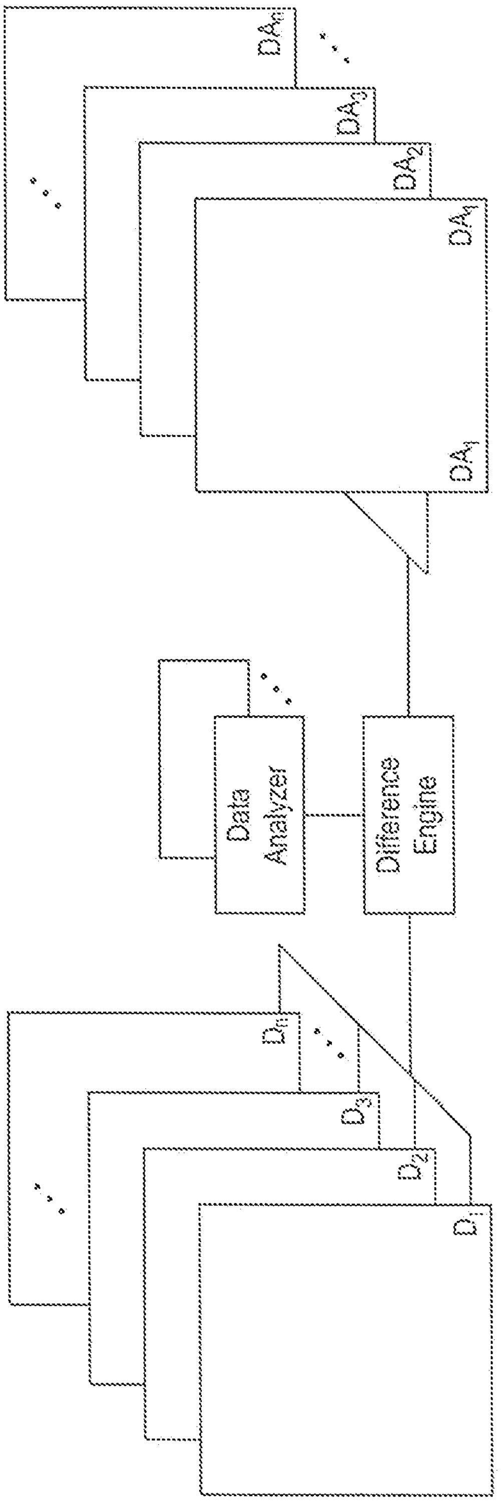

DA$_n$
DA$_3$
DA$_2$
DA$_1$
DA$_1$
Data Analyzer
Difference Engine
D$_n$
D$_3$
D$_2$
D$_1$

FIG. 10

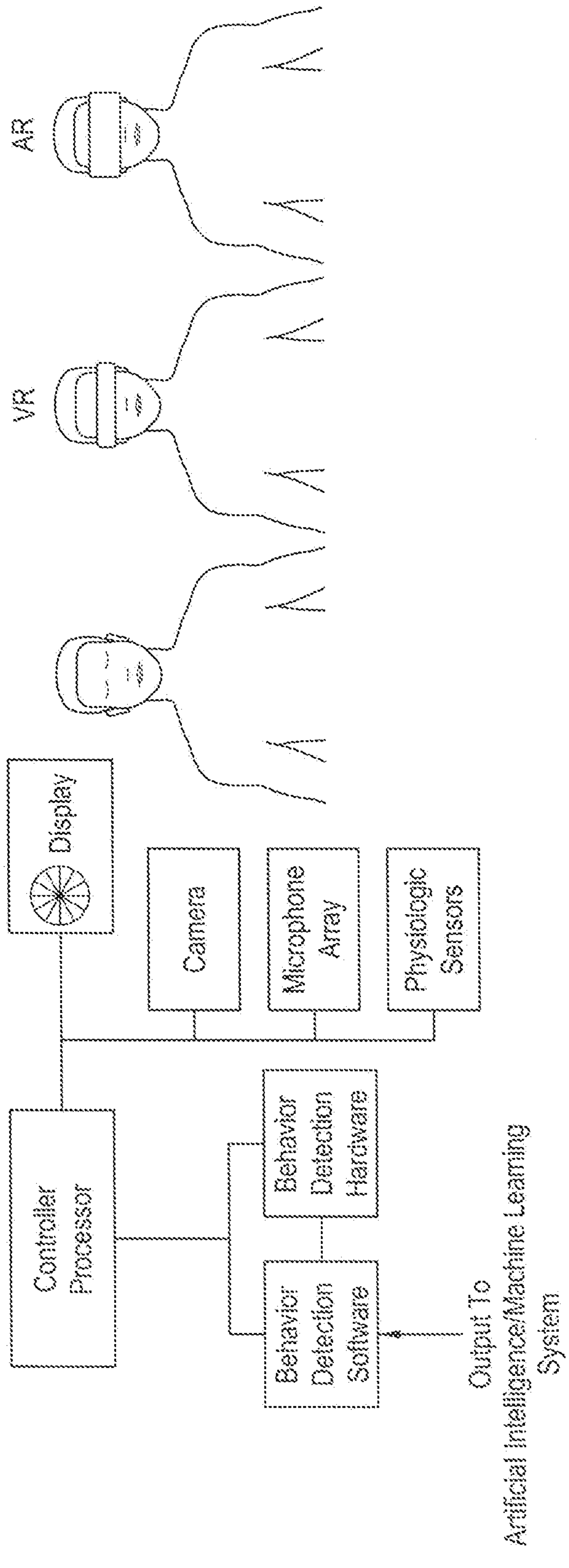
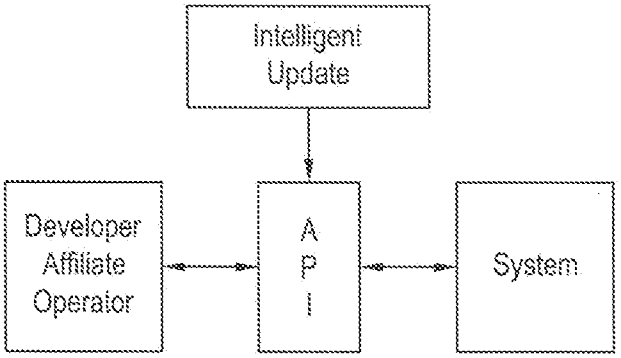
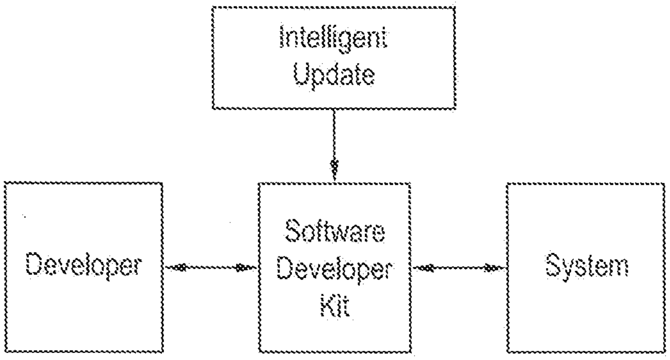

Controller Processor
Display
Camera
Microphone Array
Physiologic Sensors
Behavior Detection Hardware
Behavior Detection Software
Output To Artificial Intelligence/Machine Learning System
VR
AR

FIG. 11



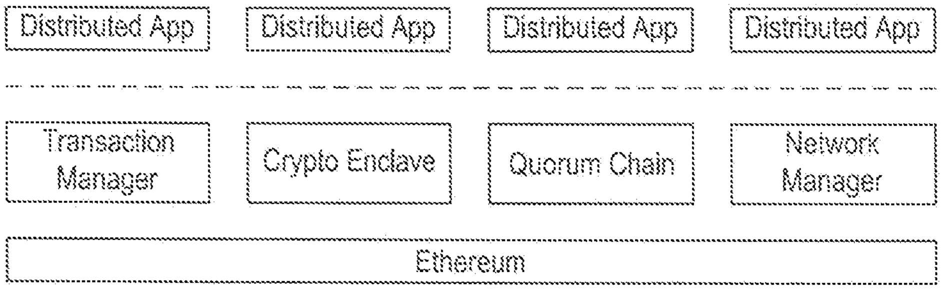
Dynamic Systems d-API

FIG. 12



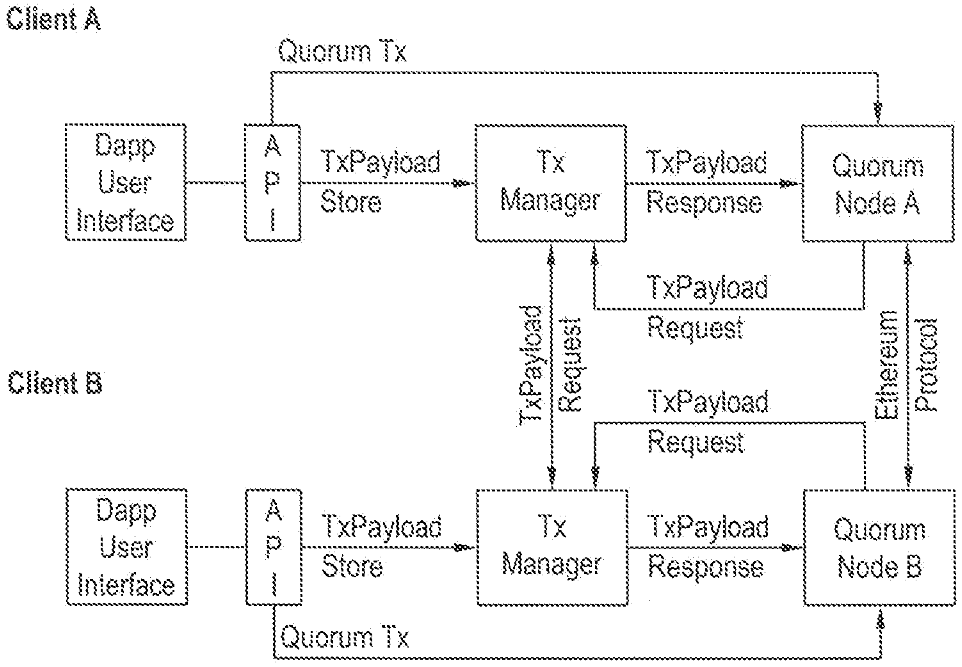
Dynamic Systems d-SDK

FIG. 13



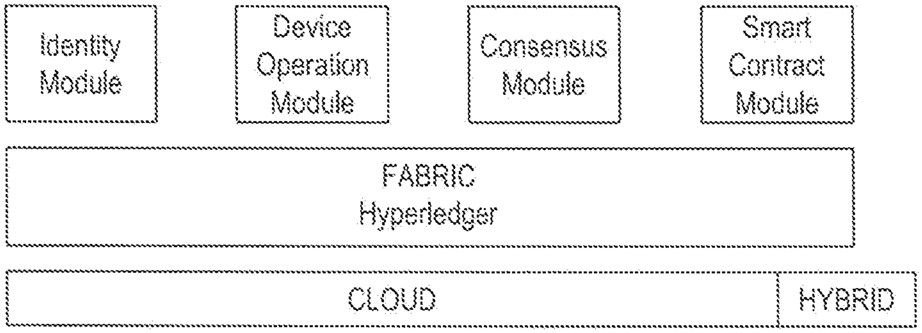
Architecture

FIG. 14



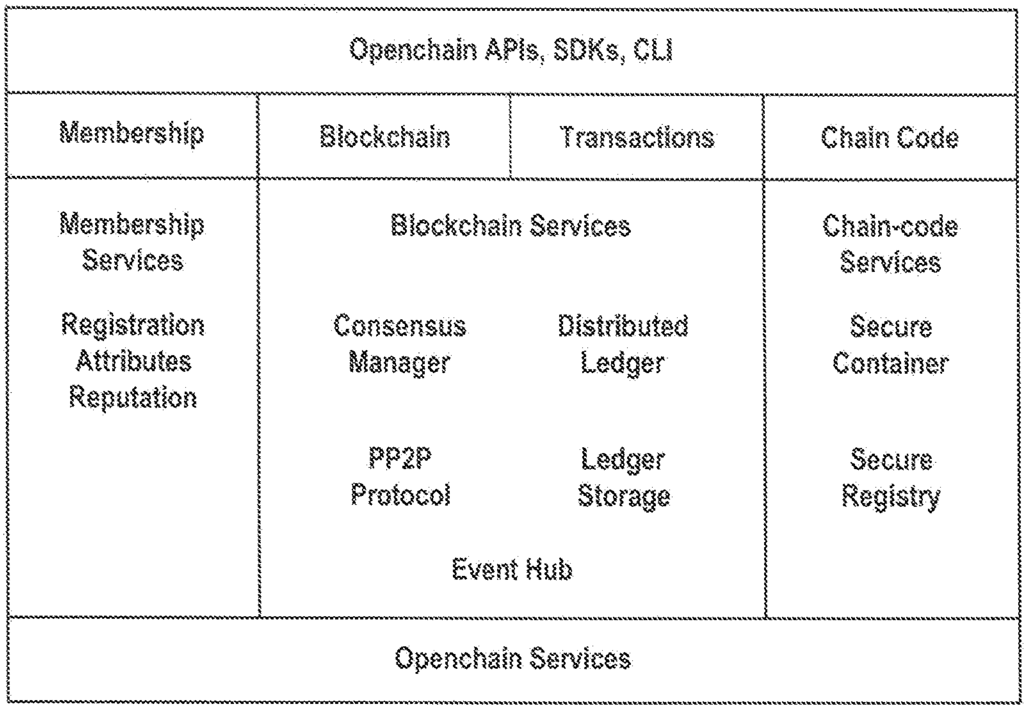
Permissioned System

FIG. 15



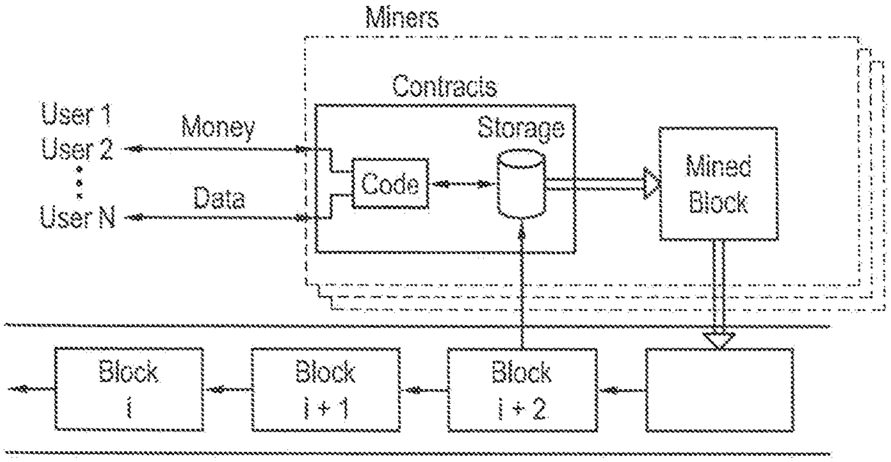
Blockchain Platform

FIG. 16



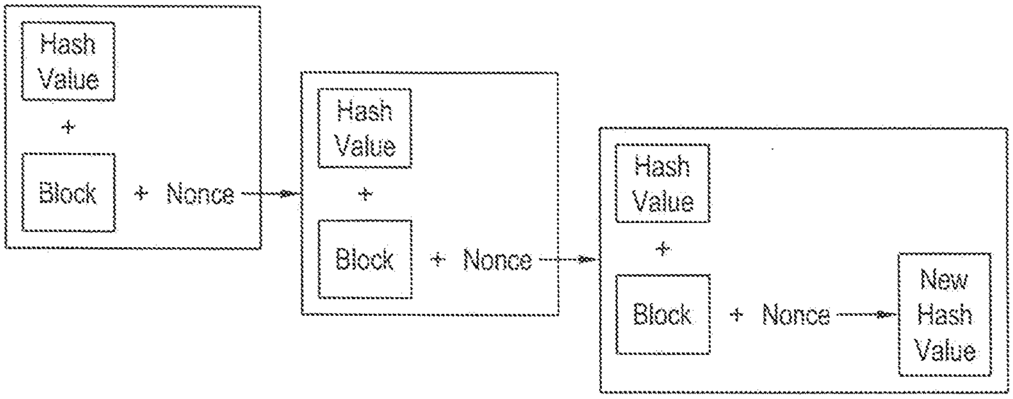
Platform

FIG. 17



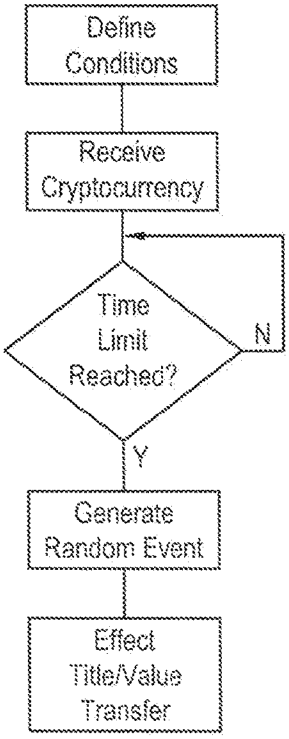
Schematic of a Decentralized Cryptocurrency System
with Smart Contracts

FIG. 18



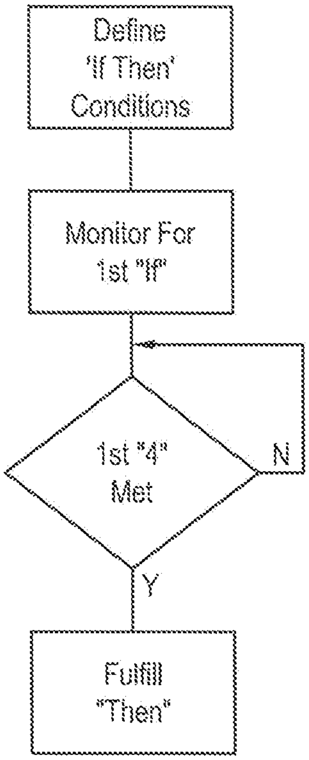
Schematic of Sequential Hash Value Creation
(Hash Value Plus Block Plus Nonce ~> New Hash Value)

FIG. 19



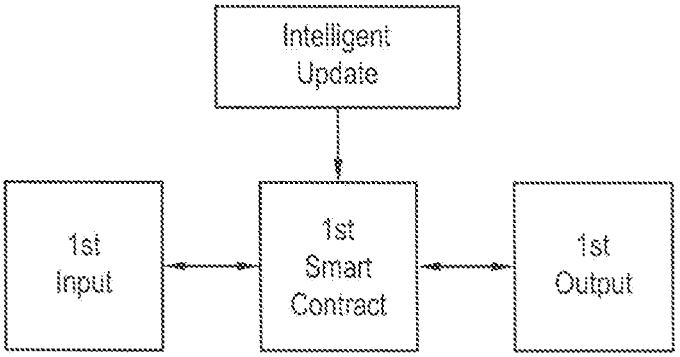
Flowchart for Crypto Currency Lottery

FIG. 20



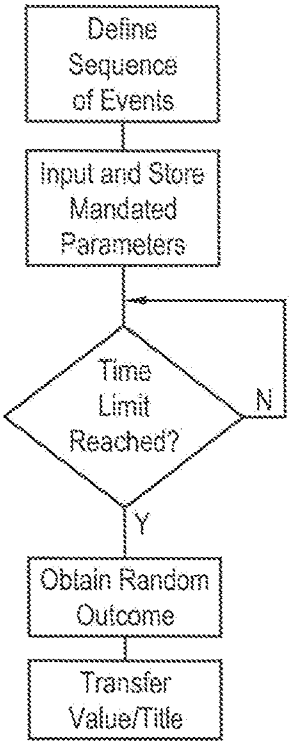
Smart Contract

FIG. 21



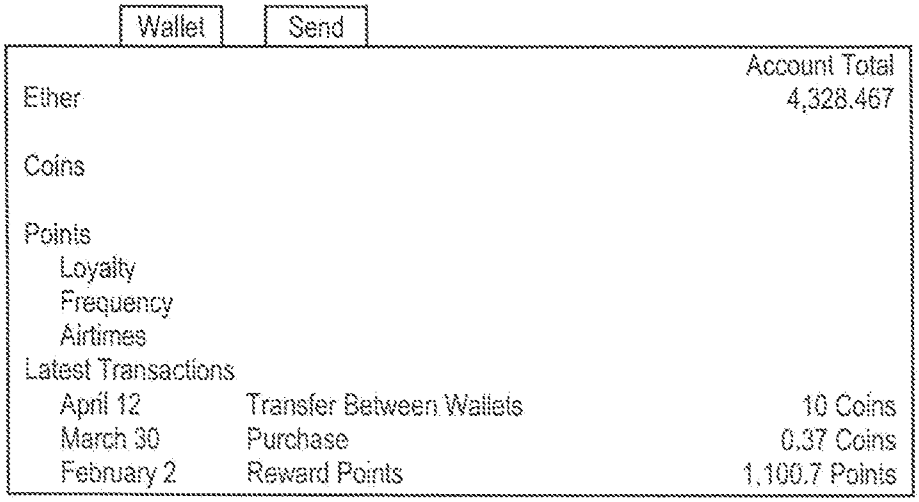
Smart-Smart (Smart^2) Contracts

FIG. 22



Smart Contracts with Mandated and Variable Parameters

FIG. 23



Account Total

Ether 4,328.467

Coins

Points

Loyalty

Frequency

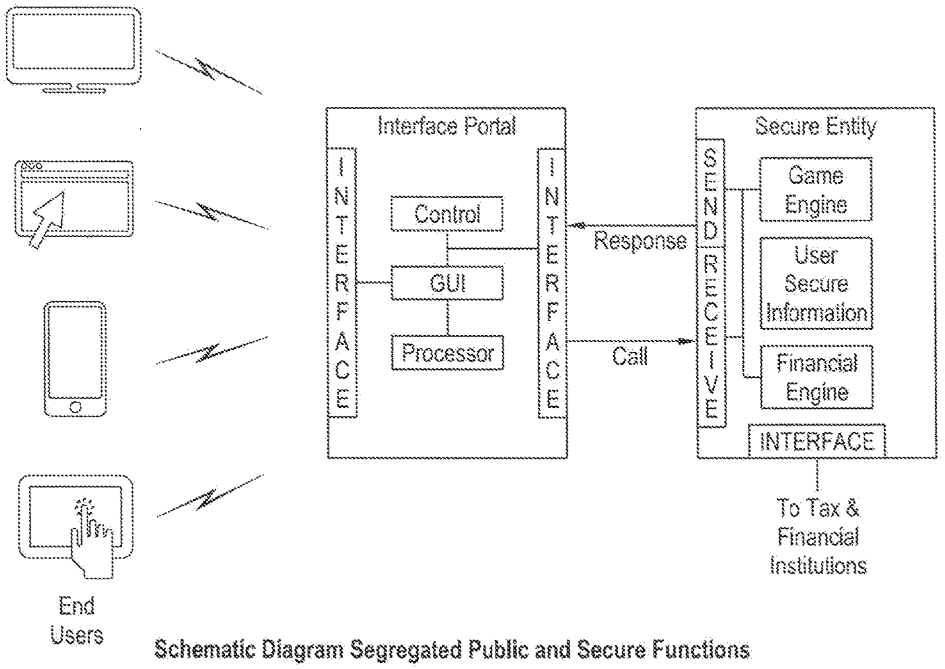
Airtimes

Latest Transactions

April 12	Transfer Between Wallets	10 Coins
March 30	Purchase	0.37 Coins
February 2	Reward Points	1,100.7 Points

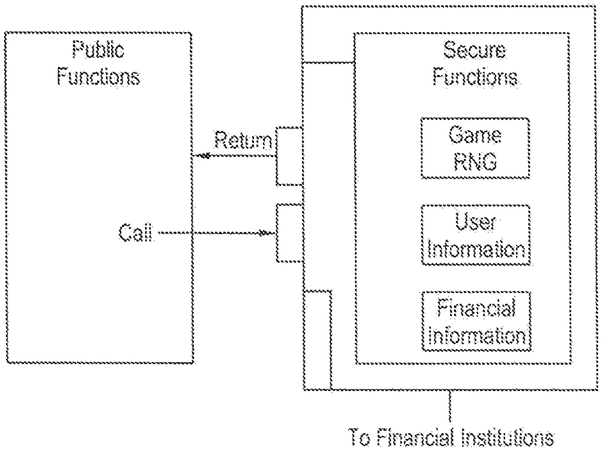
Cryptocurrency Wallet

FIG. 24



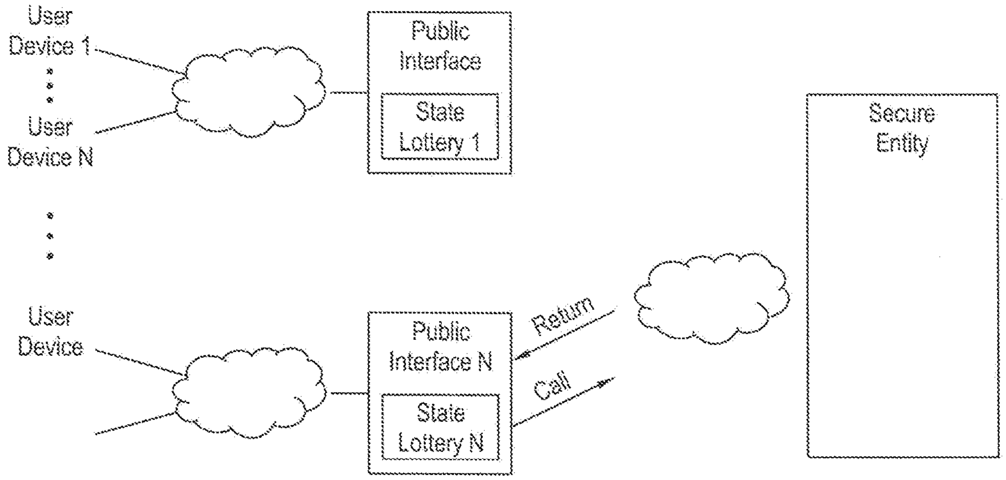
Schematic Diagram Segregated Public and Secure Functions

FIG. 25



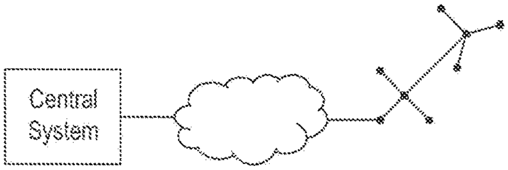
Interface of Segregated Secure and Public Functions

FIG. 26



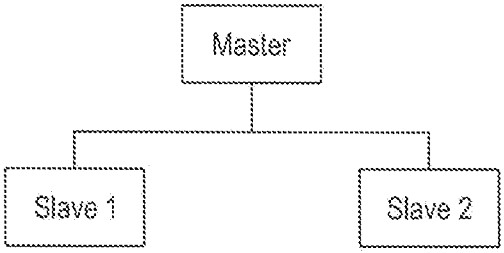
Network Implementation of Segregated Secure and Public Functions

FIG. 27



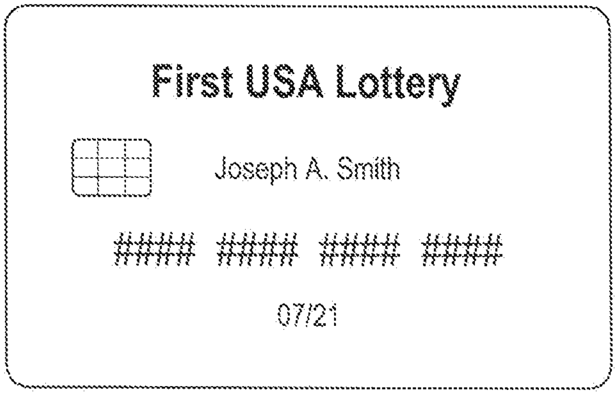
Centralized + Decentralized Systems

FIG. 28



Hierarchical Systems

FIG. 29



Lottery Linked Credit Card

FIG. 30

ARCHITECTURES, SYSTEMS AND METHODS FOR PROGRAM DEFINED ENTERTAINMENT STATE SYSTEM, DECENTRALIZED CRYPTOCURRENCY SYSTEM AND SYSTEM WITH SEGREGATED SECURE FUNCTIONS AND PUBLIC FUNCTIONS

PRIORITY CLAIM

[0001] This application claims priority to U.S. Provisional filing 62/454,423, filed Feb. 3, 2017, entitled “Architectures, Systems and Methods For Program Defined Entertainment State System, Decentralized Cryptocurrency System, and System with Segregated Secure Functions and Public Functions.

FIELD OF THE INVENTION

[0002] The present inventions relate to architectures, systems and methods for programmatically controlled entertainment state systems. More particularly, architectures, systems and methods for program control utilizing cognitive computing, including but not limited to artificial intelligence and machine learning, and optionally including analytics. Systems, methods and architectures are provided for game and entertainment operations are provided utilizing decentralized systems, including blockchain, optionally in peer to peer systems. More particularly, systems and methods for implementing a lottery, game or entertainment utilizing cryptocurrency, such as bitcoin, in a decentralized system.

BACKGROUND OF THE INVENTION

[0003] History shows that many trusted systems have evolved in order to provide for efficient functioning of society and business. Generally, these have involved central control of systems in order to ensure compliance with rules. Within the gaming space, examples include lotteries and regulated gaming. By way of example, the Nevada Gaming Control Board monitors institutions within the state for compliance with laws and regulations. and ensures the fair and efficient functioning of the industry.

[0004] Consider the entertainment and gaming system background. A lottery is a ‘State’ Function and serves as a form of ‘trusted agent’. The classic definition of the elements of a lottery are prize, chance and consideration. When these elements are reordered into a more chronologically correct order, namely first, receipt and holding of the consideration (e.g., ticket purchases), chance (e.g., ensuring a fair and accurate random number generator) and prize (i.e., paying the prize to the true winner.) Therefore, the State acts as a ‘trusted agent’ as it holds the consideration, guarantees randomness of the ‘chance’, and pays out the prize (title transfer). ‘Trust’ is based on the Integrity and Trustworthiness of People Operating the System and the Regulators Who Oversee the System. Lotteries or State Regulators are often former law enforcement. The degree of trust in the Regulators is often based on time and track record, e.g., the State of Nevada Regulatory system is considered highly trustworthy and effective, based in part on a multi-decade long track record. Additionally, a State with the most business to lose from a loss of trust in the regulatory process is most motivated to provide regulation. Such systems are based on central control of the system.

[0005] A casino is a ‘state regulated’ function and a form of ‘trusted agent’ with ‘verification’. They are licensed by the State and subject to state inspection.

[0006] Various advancements have been made in the gaming and entertainment environment. The following are assigned to the assignee of this, and are hereby incorporated by Reference as if fully set forth herein: Games, And Methods For Improved Game Play In Games Of Chance And Games Of Skill, U.S. Pat. No. 6,565,084, Games, and Methods and Apparatus for Game Play in Games of Chance, U.S. Pat. No. 6,488,280, Games, and Methods and Apparatus for Game Play in Games of Chance, U.S. Pat. No. 6,811,484, Apparatus and Method for Game Play in an Electronic Environment, U.S. Pat. No. 8,393,946, Apparatus, Systems and Methods for Implementing Enhanced Gaming and Prizing Parameters in an Electronic Environment, U.S. Pat. No. 7,798,896, Apparatus, Systems and Methods for Implementing Enhanced Gaming and Prizing Parameters in an Electronic Environment, U.S. Pat. No. 8,241,110, Methods and Apparatus for Enhanced Play in Lottery and Gaming Environments, U.S. Pat. No. 8,727,853, Methods and Apparatus for Enhanced Interactive Game Play in Lottery and Gaming Environments, U.S. Pat. No. 8,241, 100, Method and System for Electronic Interaction In A Multi-Player Gaming System. U.S. Pat. No. 8,535,134. Generally, they comprise a suite of tools to make systems more engaging, and to optimize results.

[0007] One vexing problem in larger systems results from systems incompatibility. Various components often come from various vendors. There is often a lack of interoperability and incompatibility. Various systems in the gaming ecosystem need to interoperate, including but not limited to: gaming operations, marketing, CRM (Customer Relationship Management), loyalty programs, Ancillary Points or Credits, System Analytics and Optimization, and account and audit functions.

[0008] Software Defined Systems are a collection of modules interoperated under a higher level of software control. These manage network services through abstraction of lower level functionality. Generally, there is an Application Plane, a Control Plane and a Data Plane. Examples include Software Defined Networks having a Control Plane which provides intelligent control of data plane composed of relatively less intelligent switches, routers, storage. Yet another example is software defined radio. The control plane monitors and supervises use of frequency bands in the data plane.

[0009] Yet another component is the use of static interfaces and tools. For example, APIs or Application Programming Interfaces generally comprise a static interface. They define a format for an information request. ‘If you ask for X in a specific way, we will provide Y’. Generally, no access is provided by requestor to the system other than via API. Yet another system are SDKs or Software Development Kit. They may be static. Tools are provided to achieve desired results. GDKs or Game Development Kit also may be static and provide tools for game development.

[0010] The design of entertainment or games is often driven by metrics driven design. This often involves A/B Testing comparing the results or favorability as between multiple systems. Further, they often monitor multivariate response systems.

[0011] One aspect of lotteries and Lotto style games is that they tend to be static. At the most extreme example, they are literally printed on cardstock. More generally, once a format for a lottery game has been chosen, such as a 6 out of 49 format, it is difficult to change. Public perception of change is that the game has become less favorable to the player.

[0012] Problem gambling issues have plagued the gaming industry. It is a significant issue for society. While users can solicit help (e.g., 1-800-Gambling), there is often denial and an unwillingness to seek help. Various attempts have been made to limit abuse, such as use rate limits in some on-line games.

[0013] In the move from bricks and mortar to on-line and cyber spheres, identity issues proliferate. Issues include: are you who you purport to be and will the user's identity be compromised?

[0014] Significant advances have been made in cognitive intelligence and adaptive intelligence. For example, IBM Watson won a Jeopardy competition 2011 against highly skilled players. Deep learning and pattern recognition has occurred. Current trends include big data, pattern recognition and machine learning.

[0015] Recent advances have also been made in object detection, both in 2D and 3D space. A challenge in the Large Scale Visual Recognition Challenge (LSVRC) provides for Object Detection in ImageNet 2016. The error rate of automatic labeling of ImageNet declined to less than 3%, compared to human performance of about 5%.

[0016] Significant advances have also been made in machine based game play performance. In 2015, Google DeepMind used an artificial intelligence reinforcement learning system to learn how to play 49 Atari games. In 2016, AlphaGo system from Google DeepMind beat one of the world's greatest Go players 4-1. In 2017, Carnegie Mellon University's Libratus program defeated top human players in a statistically significant manner.

[0017] Further advances have been made in cloud based systems. Functions have been migrating from local servers and storage to remote 'cloud' storage. These systems provides for easy scalability. Clouds based systems may run multiple 'instances' simultaneously. They also may combine software as a service, including Artificial Intelligence ("AI").

[0018] The Internet of Things ("IoT") utilizes devices capable of sending data to remote location, and receiving command data. Various voice controlled devices use AI or machine learning ("ML"), e.g., Amazon Alexa, Google Dot.

[0019] FIG. **1** shows an exemplary prior art centralized system. FIG. **2** shows an exemplary prior art distributed system.

[0020] Advancements have been made in trusted distributed systems such as in the use of blockchain based systems. The initial disclosure of the blockchain technology is attributed to Satoshi Nakamoto in a paper published October, 2008. This system provides for automatic trust or system trust. The blockchain paradigm provides for a decentralized system utilizing decentralized consensus. This can be done in a peer-to-peer manner without an intermediary. The system may be viewed as a network of nodes running software on a programmable distributed network. It is sometimes referred to as a transaction singleton machine with shared state, a transaction based state machine, a message passing framework, a trustful object messaging compute framework and trusted computing.

[0021] A decentralized consensus is established by a combination of blockchain and cryptography. Authority and trust is provided by the decentralized virtual network. Consensus logic is generally separate from the application. It may comprise the first layer of a decentralized architecture.

[0022] Blockchain utilizes a distributed ledger. A 'block' comprises a new group of accepted transactions. A batch of transactions is released in a block to be validated by the network of participating computers. Continuous, sequential transaction record on a public block creates a unique "chain" or blockchain. This block is published to all other nodes. The publication occurs periodically, e.g. every 10 minutes.

[0023] Etherium is an open source platform for smart contracts. As currently operated, Etherium is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference. The applications run on a custom built blockchain, an extremely powerful shared global infrastructure that can move the value and represent ownership of the property. This allows developers to create markets, store debt or promise records, move funds according to long-standing instructions (such as a will or a futures contract), without the counterparty risk. Etherium also states that its goal is to create a tradeable digital token that can be used as a currency, a representation of an asset, a virtual share, a proof of membership or anything at all. These tokens use a standard coin API, so the contract will be automatically compatible with any wallet, other contract or exchange also using this standard. The total amount of tokens in circulation can be set to a simple fixed amount or fluctuate based on any programmed ruleset. In summary, Etherium states that it enables building a tradeable token with a fixed supply, a central bank that can issue money and a puzzle-based cryptocurrency.

[0024] There are many disadvantages to the current systems. They are slow to change and innovate. They often involve proprietary systems that do not interoperate. There is often governmental and or institutional bias. There may be a cumbersome regulatory environment. Finally, there are often high transaction costs.

[0025] Thus, there is a need for interoperability among inconsistent, often proprietary systems. There is a need for gambling limitation on a more global basis, including geolimitation and global use rate monitoring for problem gambling. There is a need for problem gambling detection and remediation. There is a need for improved distributed systems.

SUMMARY OF THE INVENTION

[0026] Systems and methods are provided for training an artificial intelligence system including the use of one or more human subject responses to stimuli as input to the artificial intelligence system. One or more displays are oriented toward the human subjects to present the stimuli to the human subjects. One or more detectors serve to monitor the reaction of the human subjects to the stimuli, the detectors including at least motion detectors, the detectors providing an output. An analysis system is coupled to receive the output of the detectors, the analysis system providing an output corresponding to whether the reaction of the human subjects was positive or negative. A neural network utilizes the output of the analysis system to provide a positive weighting for training of the neural network when the output of the analysis system was positive, and a negative weighting for training of the neural network when the output of the analysis system was negative.

BRIEF DESCRIPTION OF THE DRAWINGS

[0027] FIG. **1** is a diagrammatic view of a prior art centralized system.

[0028] FIG. **2** is a diagrammatic view of a prior art centralized system.

[0029] FIG. **3** is a system level block diagram of the program defined entertainment state system (PD-ESS) showing the application plane, the control plane and the state data plane.

[0030] FIG. **4** is a system level block diagram explosion of the application state plane layer of the PD-ESS).

[0031] FIG. **5** is a system level block diagram explosion of the control plane layer of the PD-ESS).

[0032] FIG. **6** is a system level block diagram explosion of the state data plane layer of the PD-ESS).

[0033] FIG. **7** is a diagrammatic view of the ecosystem, including interfaces and interconnections.

[0034] FIG. **8** is a system level block diagram of the neural network model architecture including graphical processing units (GPUs).

[0035] FIG. **9** is a system level block diagram of the neural network model architecture.

[0036] FIG. **10** is a system level diagram of multiple data sets including a difference engine and data analyzer.

[0037] FIG. **11** is response system display and detection system for generating input to train the artificial intelligence (AI) and machine learning (ML) systems.

[0038] FIG. **12** is a system level diagram of a dynamic system application programming interface (d-API).

[0039] FIG. **13** is a system level diagram of a dynamic software development kit (d-SDK).

[0040] FIG. **14** is a system architecture level diagram of a distributed system including blockchain and Etherium.

[0041] FIG. **15** is a system architecture level diagram of a permissioned blockchain system.

[0042] FIG. **16** is a system architecture level diagram of a blockchain platform.

[0043] FIG. **17** is a system architecture level diagram of a blockchain platform including open chain services.

[0044] FIG. **18** is a system architecture level diagram of a decentralized cryptocurrency system with smart contracts.

[0045] FIG. **19** is a system architecture level diagram of a decentralized system with sequential hash value creation.

[0046] FIG. **20** is a flowchart diagram of a cryptocurrency lottery.

[0047] FIG. **21** is a flowchart diagram of a smart contract.

[0048] FIG. **22** is a flowchart diagram of a smart-smart (smart^2) contract.

[0049] FIG. **23** is a flowchart diagram of a smart contract having mandated and variable parameters.

[0050] FIG. **24** is a graphical user interface (GUI) of a cryptocurrency wallet.

[0051] FIG. **25** is a system architecture level schematic diagram of a system having segregated public and secure functions.

[0052] FIG. **26** is a system architecture level of an interface of segregated public and secure functions.

[0053] FIG. **27** is a system architecture level of a network implementation of a system having segregated public and secure functions.

[0054] FIG. **28** is a system architecture level of a combined centralized and decentralized system.

[0055] FIG. **29** is a system architecture level of a hierarchical system.

[0056] FIG. **30** is a plan view of a lottery linked credit card.

DETAILED DESCRIPTION OF THE INVENTION

[0057] Architectures, Systems and Methods for Program Defined Entertainment State Systems.

[0058] The following description is primarily in connection with FIGS. **3**, **4**, **5** and **6**, but may apply to other figures as well. An architecture is provided for a program defined entertainment state system. This preferably serves to decouple the system that controls the overall experience from the underlying systems that define states. The first plane, the application plane provides an interface, primarily for system side users, e.g., developers, organizers of events, contests, lotteries. The second plane, the control plane, provides for intelligent control, especially cognitive computing, including artificial intelligence and/or machine learning, including artificial intelligence where the system learns over time. This preferably provides an intelligent control layer above modules. The third plane, the state data plane, provides for entertainment 'state modules' with various mechanics, preferably including 'core loop', meta states and provides interfaces for end users, as well as inputs and outputs.

[0059] FIG. **3** provides a block Diagram Program Defined Entertainment State System (PD-ESS). FIG. **4** is an Explosion of PD-ESS Application Plane Layer, including an application layer GUI (facing the Developers, Affiliates, and Charities). FIG. **5** provides an Explosion PD-ESS controller plane layer. FIG. **6** provides an explosion PD-ESS state data plane layer. Also included are an explosion of entertainment state network element layer, a user interface GUI, an explosion of value/title transfer network element and explosion of other functional blocks.

[0060] Turning first to the Application Plane Layer, a program serves to communicate requirements and desired behavior to the PD-ESS Controller. It provides communication between the PD-ESS Application and PD-ESS Controller via the PD-ESS Application Controller Interface (ACI). Application Logic and Drivers are optionally provided. The application layer may receive an abstracted view of State Data Plane Actions. The PD-ESS Applications may interface with higher levels of abstracted control. The system includes an interface, the PD-ESS Application Controller Interface (ACI). The management and administration preferably provides the following: (1) To/From Application Plane, it provides contracts and SLAs, (2) To/from Control Plane Configure Policy, Monitor Performance, and (3) To/From Data Plane Element Setup.

[0061] Turning second to the Control Plane Layer, the PD-ESS Controller is ideally logically centralized entity, preferably serves to translate the requirements of the PD-ESS Application to the State Data Plane layer, and provides the Application layer with actions in the State Data Plane (e.g., event information and statistical information). The control plane may provide statistics, events and states from the Data Plane to the Application Plane. The control plane preferably enforces behavior at a low level control in the data plane, provides capability discovery, and monitors statistics and faults. The control plane advantageously includes cognitive computing, such as artificial intelligence (AI) and machine learning (ML), to be described in greater detail, below.

[0062] The control plane may optionally include analytics, including but not limited to pattern recognition. Analytics may be performed on a population, preferably a relevant population, or on a subset. Preferably, the subset has similar characteristics of a target user. Data may be binned according to subset. The scope of primary data may be analyzed. Predictive modeling may be included. Responsible Gaming Control may be implemented at the control plane level, especially if there are use rate limits and global limits.

[0063] Turning thirdly to the state data plane layer, it preferably includes main subcomponents and Functional Network Elements. Optionally, the functional network elements include some or all of the following. 1. Entertainment State Network Elements, 2. Value/Title Transfer Network Element, 3. Game Library, such as Casino, VLT, Video Gaming, Tournament, Amusement with Prize (AWP), Game Mechanics, Core Loop, Skill, Skill with Reveal, Second Chance, Social, Gamification, Prizing, vGLEPs and Prize Board, 4. Systems, Marketing, Promotions, CRM, Operations, Logistics, Interactive, Mobile/Apps and Responsive Design, 5. Platforms, 6. Channels, 7. Lottery, including Retail and Central Systems, 8. Loyalty, 9. Responsible Gaming Control, optionally including use rate limits and global limits (may be done in the control plane layer as well). 10. Sports, including real world, fantasy and eSports, 11. Other Live Data Entertainment, 12. Networks, including Network communications and web services and 13. Management, including Records, Player Account Management, Reporting, Compliance, including regulatory compliance, security, including cybersecurity, fraud and risk management, including preferably audit and payment.

[0064] The Entertainment State Network Elements provide an interface for interaction with a user of the system. An input receives information from user selection. Sensors may be of various forms, including sound sensors, motion sensors, whether 2-d or 3-d, such as including the Microsoft Kinect system. 'Internal Data' consists of data related primarily to game operations. 'External' Data sources to combine with Primary Data Source. These may include 1. Location, 2. Current Activity such as Driving (provided by vehicle, provided by tracked phone) or Exercising (provided by FitBit or similar), 3. Economic Conditions, 4. Weather, 5. Recent Events/News, e.g., a recent Large PowerBall win, 6. Marketing Information, 7. e-mail scans, e.g., Google scanning of gmail for content, 8. Social Media, and 9. the Internet of Things (IoT). The Internet of Things (IoT) provide various forms of connected devices such as data sensors. The sensors generate data input "stimuli" to system. By utilizing any form of input, the system is able to provide for massive parallelism. All data "stimuli" to system permits the system to be adaptive and reactive to all data stimuli.

[0065] An Output provides stimulation to user. Forms may include: 1. images, such on a display, or via a GUI, or VR system, AR system, 2. Thin Client display with remote computing power, 3. Projections and Holograms, 4. sounds, 5. tactile stimuli, 6. olfactory stimuli, or 7. direct electrical stimuli, neural or otherwise.

[0066] A Value/Title Transfer Network Element serves to receive and transfer value (money, coins, and other items of value). Value may refer to fungible liquid asset or other store of value. Title generally refers to ownership of real, personal, or virtual property. A detailed discussion of blockchain, trust-less, and cryptocurrency systems is provided, below.

[0067] Artificial Intelligence (AI) is broadly that branch of computer science dealing in automating intelligent behavior. They are systems whose objective is to use machines to emulate and simulate human intelligence and corresponding behavior. This may take many forms, including symbolic or symbol manipulation AI. It may address analyzing abstract symbols and/or human readable symbols. It may form abstract connections between data or other information or stimuli. It may form logical conclusions. Artificial intelligence is the intelligence exhibited by machines, programs or software. It is has been defined as the study and design of intelligent agents, in which an intelligent agent is a system that perceives its environment and takes actions that maximize its chances of success. Yet others have defined it as the science and engineering of making intelligent machines.

[0068] Artificial Intelligence often involves use of neural networks. In various embodiments, a multi-layer stack of neural network nodes are utilized. The lowest level comprises granular elements. By way of example in a gaming application, in the order of higher level understanding, the levels would progress from instances of individual action (granular), to core loop detection, to session play, to multi-session play. Optionally, a parsing engine serves to break down or subdivide a larger set, such as a data set or image, into more discrete or granular elements.

[0069] AI may have various attributes. It may have deduction, reasoning, and problem solving. It may include knowledge representation or learning. Systems may perform natural language processing (communication). Yet others perform perception, motion detection and information manipulation. At higher levels of abstraction, it may result in social intelligence, creativity and general intelligence. Various approaches are employed including cybernetics and brain simulation, symbolic, sub-symbolic, and statistical, as well as integrating the approaches.

[0070] Various tools may be employed, either alone or in combinations. They include search and optimization, logic, probabilistic methods for uncertain reasoning, classifiers and statistical learning methods, neural networks, deep feedforward neural networks, deep recurrent neural networks, deep learning, control theory and languages.

[0071] AI advantageously utilizes parallel processing and even massively parallel processing in their architectures. Graphics Processing Units (GPUs) provide for parallel processing. Current versions of GPUs are available from various sources, e.g., Nvidia, Nervana Systems.

[0072] Machine Learning is defined as a system that builds up knowledge from experience. Machine learning serves to detect patterns and laws.

[0073] Deep Learning uses Neural AI. It is easily scalable, and typically involves more layers or neural Networks (NNs). Neural Networks may be of various forms, including: efficient NN, vectorized NN, vectorized logistic regression, vectorized logistic regression gradient output, binary classification, logistic regression, logistic regression cost function, gradient descent, derivatives, computation graph and logistic regression gradient descent.

[0074] Deep neural networks (DNN) often involve hyperparameter tuning. Typically they utilize regularization and optimization. Sometimes they are referred to as Deep Belief Network (DBN)

[0075] Other forms of neural networks include Convolutional Neural Networks (CNN) or Recurrent Neural Networks (RNN). Examples of available systems include:

LSTM, Adam, Caffe, Dropout, Batch Norm, Xavier/He, Python, Scikit-Learn and TensorFlow.

[0076] AI may operate on various forms of data sets. The data set may comprise images, whether video images, 2D Data and/or 3D Data. Sequential data may be analyzed. Examples include, but are not limited to, natural language, audio, autonomous driving decisions, game states and game decisions.

[0077] Various industry applications advantageously benefit from application of AI. They include imaging and object detecting, serving to identify, classify, mining and optionally provide sentiment analysis. Other applications include autonomous driving. Yet other applications include robots and robotics. Within healthcare, functions include imaging analysis, diagnosing and gamification. Various forms of sequential data analysis may be enhanced, such as speech recognition, and natural language processing. Music applications include both recognition and synthesis. Within the gaming field, applications include game state sequences detection, analysis, formation, combination optimization, and game optimization. Chat bots and machine translation advantageously employ these systems.

[0078] FIG. **7** shows the constituent function blocks within an entertainment or gaming ecosystem. Affiliates serve to acquire customers. Affiliates receive a commission, such as based on the number of users acquired or a percent (%) of revenue. Optionally, there is a link to a credit card function (to be discussed, below).

[0079] Next are charities and other organizations that plan to operate a lottery, game or other entertainment event. They provide for customer acquisitions. They are the recipient of the event (game, lottery or entertainment). They also collect a fee.

[0080] Next are the developers, who provide for game design. In return for game design, they receive multi-jurisdictional use and payment for use. An enhanced application or app store may be provided wherein the game design may be viewed, selected and downloaded.

[0081] Next, consumers provide registration and identification information. The registration data may optionally include identification, age, address and verification. Optionally, the data is sufficient that the system can comply with Know Your Customer (KYC) rules, with optional levels of identity verification. This is stored as persistent history. The customer receives a chance to play, win, and receive entertainment.

[0082] Next is the regulator or trust verifying agent. They provide testing, approval for game fairness, overall approval, ensure compliance with regulations and security. The regulator or trust verifying agent is granted access permission by the system to monitoring of every transaction, (analytics dashboard), player accounts, parameters, prize amounts and payouts, and to the complete history. The regulator or trust verifying agent receives compensation, whether a fee or as a percentage of the transaction amounts.

[0083] Next, the lotteries serve as the trusted agent, and receive a percentage of the transaction amount. Optionally, the historical functions of the lottery may be eliminated or vaporized from the system when those functions are performed by another entity within the ecosystem.

[0084] FIGS. **8** and **9** relate to the learning processes for training neural networks. By providing repeated input stimulus and then training the neural network to provide the correct output, the system may be taught to form the correct associated output based on one or more input stimului. In converting input to the desired output the training may comprise supervised learning, such as when the target values and parameters are supervised. Alternatively, the training may be non-supervised learning, wherein the system attempts to identify patterns in the input that have identifiable structure and can be reproduced. Alternately, the system may use reinforcement learning, which works independently (like non-supervised learning) but is rewarded or punished depending on success or failure. Preferably, reinforcement learning involves incremental change. In the various training techniques, perturbation may be used wherein one or more input parameters are varied, typically in a perturbation amount, e.g., less than 10%, more preferably less than 5%, and most preferably less than 3%, of the input value, so as to monitor the effect of the perturbation on the output.

[0085] Hyperparameters and parameters may be used in the AI or machine learning systems. Model parameters are estimated from data automatically. A configuration variable internal to the model can be estimated from data. This can be required by the model when making predictions. Values define the skill of the model. They may be estimated or learned from data.

[0086] Hyperparameters are set manually and are used in the processes to help estimate parameters. A configuration variable external to the model is used. Generally, it cannot be estimated from the data. They are often used in processes to estimate model parameters. They are typically specified by the system user. Hyperparameters can often be set using heuristics. They are often tuned for a given predictive modeling problem. A hyperledger may be used, either as a hyperledger composer or hyperledger fabric.

[0087] The AI or machine learning may be performed on various types of hardware. Advantageously, systems that support parallel processing can provide for computation speed and efficiency. Parallel processing units such as Graphics Processing Units (GPUs) are available from NVIDIA and AMD. Neural Processing Units (NPUs) are available in the Kirin 970, Apple A11 and the Qualcomm Zeroth Processor. AI and machine learning processing is also available as a cloud AI or Machine learning system, such as is available from Google and Amazon Web Services.

[0088] FIG. **10** describes domain transformations and difference engines. One advantageous domain transformation involves the time domain to frequency domain (time series to frequency domain). One example is the Fourier series, which generally is used with repetitive signals, such as oscillating systems. A Fourier transform, is generally used with non-repetitive signals, such as transients. Enhanced computational techniques such as the Fast Fourier Transform (FFT) may be used for efficiency and computational speed. Yet another domain transformation is the Laplace transform, often used in electronic circuits and control systems. Yet another, the Z transform, is used with generally discrete-time signals. Digital Signal Processors (DSPs) may be advantageously utilized. Spectral density estimation may be included, along with wavelet analysis, image analysis, data compression and multivariate analysis. Correlated data sets are advantageously employed.

[0089] Difference engine may be employed to identify differences between two or more sets of data. The difference may be time based, such as where one data set relates to a time **0**, and the other set relates to a time **1**, time **2**, time **3**, . . . , time N. Differences in images may be calculated.

[0090] FIG. **11** shows a system in which the Subject response may be monitored, captured and analyzed for behavior, which is then used as input to AI. In various efforts, such as in game or entertainment design and creation, the response of the target audience may be monitored, analyzed and used to train an Artificial Intelligence or machine learning system. The subject response to entertainment/game stimuli serves to measure the 'fun' experienced by the subject, and that measure (the 'fun') is then used as a training input to AI or ML system. The system may detect individual subject behavior. Alternatively, the system may monitor group behavior, serving to detect the 'fun' experiences, but may also measure attributes of the group or crowd, such as 'excitement', 'engagement' or crowd based behavior.

[0091] A display is provided as a stimulus to the subject or subjects. A flat panel display or monitor may be utilized. Optionally, personal viewing devices may be utilized, such as individual screens, virtual reality headsets, augmented reality devices, heads up displays, projection devices or imaging technology.

[0092] Various detectors are utilized to monitor the one or more subject's response. Motion detection utilizes motion tracking hardware and software. A camera images the subjects. Various cameras include the Microsoft Kinect, 2d sensors and cameras and 3d sensors and cameras. Metrics detectors may analyze the position of a body part, such as a limb, joint or facial feature. It may measure the velocity, movement, higher level derivatives of the position or movement, such as the rate of change of change. Facial detectors monitor for facial recognition. Facial attributes may be detected, such as positive attributes, e.g., a smile, or negative attributes, e.g., a frown. Body position detection may be determined. Sound detection may be performed with a microphone or microphone array. It may detect attributes of the sound, such as positive attributes, e.g., a cheer, and negative attributes, e.g., expletives, and boos. Biometric scan detection is utilized. Physiologic response detection optionally monitors the subject heart rate, blood pressure, pupil dilation, temperature, ECG, and mental activity. Activity monitoring detectors monitor engagement response, preferably including bet rate, time spent engaged with the display, retention rate, repetition rate and reengagement rate. Analytics are advantageously utilized.

[0093] The output of the system is used as input in the AI or machine learning system. For example, in training using reinforcement learning in neural networks, a positive weighting is used for positive attributes, and a negative weighting is used for negative attributes.

[0094] The system may additionally provide output identified as associated with addiction, such as gambling addiction, or a subject otherwise being 'hooked' on the game. When the level of engagement or minor addiction is viewed as acceptable, a positive weighting may be used in the training, whereas when the addiction is viewed as unacceptable or excessive, a negative weighting may be used in the training.

[0095] The artificial intelligence, machine learning, neural network, use of user response in training AI/M L systems (generally FIG. **11** and discussion, above), may advantageously be utilized in game design and develop, entertainment development and/or any creative developmental effort.

[0096] The systems may constitute a matrix of tools. They may comprise a given set of tools. In a more fundamental way, they comprise a tool to discover the tools. Tools may be game states, entertainment states or any form of state or matter.

[0097] The following will be described as to game development, but the tools, systems, methods and architectures may be applied to entertainment or any creative effort. As to a particular game, a first option is to provide only basic rules of that given game. The system may play against itself, or alternatively, play against other systems, in order to discovery winning game play strategies. In yet another option, the system may be provided with known gambits, with the system permitted to use or ignore the gambits. In yet an alternative embodiment, the system may be provide with a library of games. The system may analyze the library of games for game elements, game mechanics or core loops. Optionally, the system may limit analysis of the library of games to similar games, or may consider all games, optionally divided into subunits, e.g. card games, board games, video games. Once the various core loops or game elements are defined, the system may combine them in various combinations and permutations so as to define a new game or game play sequence. The system may recognize patterns in the data. Values may be assigned to decisions at various points or game states or game state decision points. The use of user response may be advantageously used in game formation and optimization. The use of user response is particularly suited to reinforced learning.

[0098] The system may operate in a hierarchical manner. Hierarchical systems may be used, where it may vary a 'subservient' mandated parameter so long as 'superior' or 'master' mandated parameter is met. By way of example, a 'super' mandated parameter' may be used to guarantee a particular outcome. Alternatively, an administrative control may be granted, such as to set a 'top level' constraint.

[0099] The system may consider separate functions in a cooperative action. Functions may be reassigned or moved to other, especially lower, levels of action. The system may provide new variables. By providing a hierarchical response, core functionality may be maintained. Optionally, the system may employ a "kill switch" for the system, an apoptosis, such as based on a command such as from an administrator, or based on predefined criteria. The system may provide a package of experience ('Total Recall') such as in a continuous state and/or persistent state.

[0100] FIGS. **12** & **13** relate to various dynamic, that is changeable, systems. In the designation "d-API" and "d-SDK", 'd' stands for 'dynamic' and is capable of change within and by the system. The format of the interaction (request and/or response) may be changes. Alternately, it may change the type, quantity or quality of information provided in the response. Other factors that may be changed include the ability of the request to alter the information via the API or SDK. Changes may be made to other operational or administrative rights or permissions, such as read only access, read and write, edit rights, super administrative rights. These provide for dynamic change under adaptive control.

[0101] Within the dynamic-Application Programming Interface (d-API), an initial format for request and response is defined. This may be considered in an 'if-then' statement: IF you ask for X in an agreed upon format, THEN system will provide X. The dynamic system may vary the format, and/or response. An intelligent dynamic update may be based on AI, machine learning or analytics. While not limited to the following, some or all of these changes may be implemented dynamically: the format of the interaction (request and/or response), access to more information or functionality, e.g. read only, or modification rights, the ability to provide information or data to the system, and the ability to change data.

[0102] Within the dynamic Game Development Kit (d-GDK), an initial kit is provided. The system then permits dynamic modification of the GDK. Preferably, dynamic modification is based on AI or Machine Learning or analytics.

[0103] Dynamic Segregated Lottery (d-SL) may be provided wherein one or more functional units or the lottery may be provided. A virtualized system may be utilized, such as in the use of a virtualized server.

[0104] FIGS. **14-20** relate to a blockchain implementation for games, entertainment or other useful ends. Blockchain uses a cryptographic 'hash' to identifies each block and transaction. Each successive block contains a hash of the previous code. This permanently fixes transactions in chronological order. The blockchain utilizes both a private key and public key. The prior hash is added to the new blockchain with a nonce to form a new hash.

[0105] Cryptocurrency provides for cryptographically secure transactions. Cryptocurrency is a programmable currency or decentralized value transfer system. It is also a decentralized virtual currency or decentralized digital currency.

[0106] Proof of work, or proof of stake, is the "right" to participate in the blockchain. It must be onerous enough to prevent changes without redoing the work. Bitcoin is a created currency which is mined and serves as a reward for payment processing work. Blockchain cryptocurrency involves no transaction charges or fees paid by purchaser. There are no refund rights or chargebacks.

[0107] It may be implemented in any form of network, both public and private. Open software and proprietary software may be used. Storage may be local storage or cloud storage and computing. Analytics may be performed locally or in a cloud analytics system. Analytics As A Service (AAAS) may be performed. Systems may be permissioned v. permission less distributed systems.

[0108] FIGS. **21** through **23** relate to smart contracts. The core elements are, first, a set of promises which may be contractual or non-contractual. Second, they are specified in digital form, operate electronically, where the contractual clauses or functional outcomes embedded in code. Third, they include protocols, or technology enabled rules-based operations. Fourth, the parties perform on the promises through automated performance, in a generally irrevocable manner.

[0109] Smart contracts automate different processes and operations. In one embodiment, they automate "if-this-then-that" on self-executing basis with finality. They may provide for payments. Actions may be conditioned on a payment or payments, such as with the control of collateral based on payment.

[0110] Smart contracts may be implemented via blockchain. This forms a trusted system, which may be implemented in a business to business implementation (B to B) and/or peer-to-peer implementation. The machine-to-machine implementation permits various combinations. In one implementation, a blockchain is combined with devices comprising the Internet of Things (IoT). In yet another combination, the blockchain may be combined with devices comprising the Internet of Things in combination with artificial intelligence. Generally, the block contains smart contract program logic. It bundles together the messages relating to a particular smart contract including inputs, outputs, and logic. In yet another implementation, they may provide contracts for difference, such as in use the current market price to adjust balances and disperse cash flow.

[0111] Smart contracts are a trust shifting technology. They reduce counter-party risk. Preferably, this serves to increase credit.

[0112] Smart contracts may be implemented in various models. They may be a contract entirely in code. They may be a contract in code with separate natural language version. They may be split natural language contract with encoded performance. Alternatively, they may be a natural language contract with encoded payment mechanism.

[0113] Smart contract initiation involves a consensus. An algorithm constitutes a set of rules for how each participant in the contract processes messages. They may be implemented in a permission-less manner, wherein anyone may submit messages for processing. The submitter may be involved in consensus. Alternately, they may delegate decision making such as to an administrator or sub-group of participants. An alternative implementation is to have a permissioned system, in which the participants are limited. They are generally pre-selected. They are then subject to gated entry and be subject to the satisfaction of certain requirements and/or approval of an administrator.

[0114] Smart contracts are subject to various methods of formation. They may by agreement such as where there is a common cooperative opportunity or a defined desired outcome. These may include business practices, asset swaps, and transfer of rights. Next, conditions set for initiation of the contract. That may be by the parties themselves, or by the occurrence of some external event, such as time, other quantifiable measure or location. Typically, they generate a code, which is encrypted and chained with blockchain technology. It may be authenticated and verified. Upon execution and processing, the network updates all ledgers to indicate current state. Once verified and posted, they cannot be changed, with only additional blocks appended.

[0115] To restate, the smart contract serves as a distributed application on networks with independent built-in trust mechanisms. The program is entrusted with unit of value combined with rules for transfer of ownership of the unit of value. They serve as self-executing programs that automatically fulfill the terms of a programmed relationship.

[0116] FIG. **20** shows a Lottery embodiment implemented as a smart contract. The method for implementing a lottery includes the following steps. A time frame is set in which to receive cryptocurrency. Second, cryptocurrency is received with owner identification within the timeframe. The window opens for a specified duration, afterwards at which the window closes. The smart contract generates or receives a random event, such as from a random number generator. The random number generator should include an algorithmic guarantee of randomness and a guarantee of no hack. The contract selects a new owner (winner) among the owner identification related cryptocurrencies. It then assigns new ownership of cryptocurrency to selected new owner (winner).

[0117] Smart contract may be used to implement a core loop or a game mechanic. The following core loops and game mechanics comprise a partial list of those that may be implemented, including but not limited to JACKO, POKO, Hot Seat, Hi Lo, Rock, Paper Scissors, In the Zone and iLotto or other array or geography based game mechanics or core loops. Any subunit of the game mechanic or core loop may itself be used as a game mechanic or core loop.

[0118] Jacko is a game comprising the steps of: randomly selecting a target number from a first range of numbers having a minimum and maximum number, presenting an indication of the target number to the player, selecting a number for the player, the number being selected from a second range, having a minimum and maximum, where the maximum is equal to or less than ½ of the minimum of the first range, receiving an indication from the player whether to draw again, and if so, randomly selecting a number from the second range, accumulating the total of the player's draws, and repeating this step until either the player declines to draw or the total exceeds the target number, and in the event the player declines to draw, randomly selecting numbers from the second range, accumulating those numbers, comparing them to the player's accumulated amount, and assigning as to the winner whomever has a total closest to, but not exceeding, the target.

[0119] Poko is a multi-player game where multiple indicia are awarded a predefined value, where other players have no information as to at least some of the indicia held by other players.

[0120] High Lo is a game comprising the steps of: performing a first lottery selection of a series of randomly drawn numbers, receiving from a player an indication whether the next randomly drawn number will be higher or lower than the preceding number, and if correct, awarding winnings correlated to the amount of the randomly drawn number, and continuing until the player fails to predict the high/low outcome, or elects to stop.

[0121] In the Zone is a game of chance comprising the steps of randomly selecting a player's target number within a predefined range of numbers, the range having a minimum and a maximum, randomly selecting a series of numbers for use in a lottery game, the minimum of the predefined range of numbers being at least equal to the sum of the lowest possible total for the series of the lowest possible total for the series of numbers and the maximum of the predefined range of numbers, totaling the random selected series of numbers through the conclusion of the selection, and assigning prize amounts to players having a player's number not exceeding the total based upon the proximity of the player's number and the total number.

[0122] Rock Paper Scissors is a game with three or more options having an assigned priority of options relative to one another.

[0123] Hot Seat is a game of increasing risk/reward including the ability to 'opt out' in Smart Contract. A method for game play in a multi-level game of chance culminating in a final level, comprises the steps of presenting, at a given level, a plurality of random options wherein at least one option is a positive option, another option is a negative option, and a third option requiring a further decision, receiving a selection regarding which one of the plurality of random option is selected, and if the positive option was selected, cumulating the positive option result with the prior positive option results, but if the negative option was selected, cumulating the negative option result, comparing the cumulative result with a predetermined number, and replaying the same level if the cumulative number is less than the predetermined number or terminating the game if the cumulative number equals the predetermined number, and if the third option was selected, receiving a selection regarding the decision, respecting the above steps until the player stops, the predetermined number of negative events occurring or the final level is related.

[0124] iLotto is a grid or geography based system including a display for presenting a grid of identifying objects, an input for receiving a player selection of an identifying object, a random generator for randomly selecting a winning identifying object, and a point tally system for awarding points to the player according to the rules comprising a first point value if the player selected identifying object exactly matches the winning identifying object, a second point value if the player selected identifying object is in a geometric relationship with the winning identifying object, and a third, negative, point value if the player is not awarded the first point value or the second point value.

[0125] FIG. **23** relates to implementation of mandated and variable parameters. Mandated parameter are set in smart contract. Examples of mandated parameters include payout percentage and payout amount. Variable parameters are subject to mandated parameters, providing entertainment options.

[0126] FIG. **24** depicts a wallet serving for the electronic storage of cryptocurrency. This represents a graphical user interface, such as on a phone or computer display. Various forms of cryptocurrency may be displayed on the GUI and stored in the wallet. Points may be awarded, such as for loyalty, frequency and airtimes. Recent or latest transactions may be listed, indicating the date, purpose and amount. A total account value may be shown.

[0127] Cryptocurrency systems and smart contracts may be implemented in combination with other systems. One additional system comprises a frequent user or player's club system. They may be combined with other forms of 'currency lite', including micro-transactions and micro-payments. They may be used in combinations with smart properties, that is digital assets or physical things that know who their owner is. Digital assets are anything that exists in digital, typically binary, format and comes with the right to use. Examples include images, including still pictures and video or dynamic images, audible content, such as sounds, music or performances, and digital documents. Property whose ownership is controlled via distributed trusted network, e.g., blockchain using contracts. They may be further used in combination with geolocation, wherein the physical location (geolocation) of various components and architectural components are optionally a component of the system. Limits may be placed on the geography of game play. The system can ensure compliance with geolocation of data routing.

[0128] FIGS. **25** through **27** relate to systems having segregated secure functions and public functions. This provides a secure platform with multiple interfaces to public functions and public entities. The segregated secure functions provide the function of the trusted agent. The secure functions include one or more of the following. First, outcome determination. This may include the use of a random number generator (RNG) or probability engine. Second, user or player account information is stored. Third, monetary accounting or transactions are stored. Fourth, regulatory and compliance interface is performed. Fifth, interfaces such as a developer interface. Sixth, regulatory functions including Q&A testing, compliance, testing and approval may be provided.

[0129] The public functions include some or all of the following. First, the public system issues a 'call' to the secure system. A 'call' may be via an Application Programming Interface (API) or d-API. The "OPEN" system call makes calls to secure system for secure data. Second, a designer interface serves to access tools, APIs, a Development Kit (DK), and a Software Development Kit (SDK). Third, a marketplace interface serves as a lottery interface and optionally an application or app store. Fourth, an operator interface serves to interface with an operator or organizer, e.g., a charity. It preferably serves to publish, market, and sell. Fifth, the user interface permits registration, play activity and persistent history.

[0130] The system components may vary by function. Public interfaces and functions preferably comprise an "open" platform. This allows for arbitration and agreement with the secure entity regarding game operations to be performed by the secure entity, e.g., payout %, vGLEPs, who may play, and geolocation. The secure entity performs secure functions including game outcomes, financial matters and secure user data. The end users utilize a "channel mix", including but not limited to web, mobile app, mobile web, tablet, computer, display enabled Devices (wireless), touch screen equipment at retailer, e.g., countertop games. The private entity may impose rate limits and impose responsible gaming controls.

[0131] FIGS. **28** and **29** describe hybrid and hierarchical systems. A centralized system, such as a state run lottery may be combined with a decentralized system, such as a blockchain implementation. Hierarchical order may be imposed within the system. In a system using mandated and variable parameters, a hierarchy of mandated parameters may be established, and then various variable parameters may be subject to the appropriate mandated parameter. In another application, a global use rate limit may be imposed at a high level in the hierarchy. Hierarchical use rate limits may be imposed. Various topologies of systems include master slave, master over multiple slaves and circular systems.

[0132] FIG. **30** relates to a game or lottery linked credit card and credit card function. A credit card and credit functionality may be linked to lottery or other game play. Through use of the credit card, a conversion rate is established. By way of example, for every $100 of purchases, $1 in lottery play is made. The rate may be variable, such as based upon institution. In the event a charitable organization organized or sponsored the lottery or game, every $100 of purchases accrues $2 for the organization. A split may also be performed, such as for every $100 of purchases accrues $1 in the lottery or game for the credit card owner and $1 for the organization.

[0133] In alternative embodiments, the mobile gaming device may be connected to the gaming machine with a cable, either directly connected to a port of the gaming machine or via a network communicating with the gaming machine.

[0134] The software used to program the gaming machines and servers in accordance with the embodiments described herein may be initially stored on a ROM, such as a CD or an electronic memory device. Such CDs and devices are non-transitory computer readable mediums having the appropriate computer instructions stored thereon. The programming may also be downloaded to the gaming machines via the casino's network.

[0135] The software used to program the gaming machines and servers in accordance with the embodiments described herein may be initially stored on a ROM, such as a CD or an electronic memory device. Such CDs and devices are non-transitory computer readable mediums having the appropriate computer instructions stored thereon. The programming may also be downloaded to the gaming machines via the casino's network.

[0136] It should be appreciated that the terminals, processors, or computers described herein may be embodied in any of a number of forms, such as a rack-mounted computer, a desktop computer, a laptop computer, or a tablet computer. Additionally, a computer may be embedded in a device perhaps not generally regarded as a computer but with suitable processing capabilities, including an electronic gaming machine, a Web TV, a Personal Digital Assistant (PDA), a smart phone or any other suitable portable or fixed electronic device.

[0137] Also, a computer may have one or more input and output devices. These devices can be used, among other things, to present a user interface. Examples of output devices that can be used to provide a user interface include printers or display screens for visual presentation of output and speakers or other sound generating devices for audible presentation of output. Examples of input devices that can be used for a user interface include keyboards, and pointing devices, such as mice, touch pads, and digitizing tablets. As another example, a computer may receive input information through speech recognition or in other audible formats.

[0138] Such computers may be interconnected by one or more networks in any suitable form, including as a local area network or a wide area network, such as an enterprise network or the Internet. Such networks may be based on any suitable technology and may operate according to any suitable protocol and may include wireless networks, wired networks or fiber optic networks. As used herein, the term "online" refers to such networked systems, including computers networked using, e.g., dedicated lines, telephone lines, cable or ISDN lines as well as wireless transmissions. Online systems include remote computers using, e.g., a local area network (LAN), a wide area network (WAN), the Internet, as well as various combinations of the foregoing. Suitable user devices may connect to a network for instance, any computing device that is capable of communicating over a network, such as a desktop, laptop or notebook computer, a mobile station or terminal, an entertainment appliance, a set-top box in communication with a display device, a wireless device such as a phone or smartphone, a game console, etc. The term "online gaming" refers to those systems and methods that make use of such a network to allow a game player to make use of and engage in gaming activity through networked, or online systems, both remote and local. For instance, "online gaming" includes gaming activity that is made available through a website on the Internet.

[0139] Also, the various methods or processes outlined herein may be coded as software that is executable on one or more processors that employ any one of a variety of operating systems or platforms. Additionally, such software may be written using any of a number of suitable programming languages and/or programming or scripting tools, and also may be compiled as executable machine language code or intermediate code that is executed on a framework or virtual machine.

[0140] In this respect, embodiments may provide a tangible, non-transitory computer readable storage medium (or multiple computer readable storage media) (e.g., a computer memory, one or more floppy discs, compact discs (CD), optical discs, digital video disks (DVD), magnetic tapes, flash memories, circuit configurations in Field Programmable Gate Arrays or other semiconductor devices, or other non-transitory, tangible computer-readable storage media) encoded with one or more programs that, when executed on one or more computers or other processors, perform methods that implement the various embodiments discussed above. The computer readable medium or media can be transportable, such that the program or programs stored thereon can be loaded onto one or more different computers or other processors to implement various aspects as discussed above. As used herein, the term “non-transitory computer-readable storage medium” encompasses only a computer-readable medium that can be considered to be an article of manufacture or a machine and excludes transitory signals.

[0141] The terms “program” or “software” are used herein in a generic sense to refer to any type of computer code or set of computer-executable instructions that can be employed to program a computer or other processor to implement various aspects of, as discussed above. Additionally, it should be appreciated that according to one aspect of this embodiment, one or more computer programs that when executed perform methods need not reside on a single computer or processor, but may be distributed in a modular fashion amongst a number of different computers or processors to implement various aspects of embodiments described herein.

[0142] Computer-executable instructions may be in many forms, such as program modules, executed by one or more computers or other devices. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Typically the functionality of the program modules may be combined or distributed as desired in various embodiments.

[0143] Also, data structures may be stored in computer-readable media in any suitable form. For simplicity of illustration, data structures may be shown to have fields that are related through location in the data structure. Such relationships may likewise be achieved by assigning storage for the fields with locations in a computer-readable medium that conveys relationship between the fields. However, any suitable mechanism may be used to establish a relationship between information in fields of a data structure, including through the use of pointers, tags, addresses or other mechanisms that establish relationship between data elements.

[0144] Various aspects of embodiments described herein may be used alone, in combination, or in a variety of arrangements not specifically discussed in the embodiments described in the foregoing and the concepts described herein are therefore not limited in their application to the details and arrangement of components set forth in the foregoing description or illustrated in the drawings. For example, aspects described in one embodiment may be combined in any manner with aspects described in other embodiments.

[0145] Also, embodiments described herein may provide a method, of which an example has been provided. The acts performed as part of the method may be ordered in any suitable way. Accordingly, embodiments may be constructed in which acts are performed in an order different than illustrated, which may include performing some acts simultaneously, even though shown as sequential acts in illustrative embodiments.

[0146] While embodiments have been described with reference to certain exemplary features thereof, those skilled in the art may make various modifications to the described embodiments. The terms and descriptions used herein are set forth by way of illustration only and not meant as limitations. In particular, although embodiments have been described by way of examples, a variety of devices would practice the inventive concepts described herein. Embodiments have been described and disclosed in various terms, the scope of the embodiments is not intended to be, nor should it be deemed to be, limited thereby and such other modifications or embodiments as may be suggested by the teachings herein are particularly reserved, especially as they fall within the breadth and scope of the claims here appended. Those skilled in the art will recognize that these and other variations are possible as defined in the following claims and their equivalents. Although the foregoing invention has been described in some detail by way of illustration and example for purposes of clarity and understanding, it may be readily apparent to those of ordinary skill in the art in light of the teachings of this invention that certain changes and modifications may be made thereto without departing from the spirit or scope of the appended claims.

[0147] All publications and patents cited in this specification are herein incorporated by reference as if each individual publication or patent were specifically and individually indicated to be incorporated by reference in their entirety.

REFERENCES

[0148] ARM, IBM, “The Internet of Things Business Index 2017, Transformation In Motion”, The Economist, Intelligence Unit Limited 2017, pages 1-22.

[0149] Crosby, et al., “Blockchain Technology: Beyond Bitcoin”, Applied Innovation Review, Issue No. 2, Sutardja Center for Entrepreneurship & Technology, Berkeley Engineering, June 2016, pages 1-19.

[0150] Fisher, “Decentralized Peer to Peer Game Assets Platform, Integration with Third Party Games using Smart Contract,” https://bravenewcoin.com/assets/Whitepapers/. BitSharesPlayWhitePaper-EN.pdf. Aug. 4, 2014. 12 pages.

[0151] Hinton et al., “A Fast Learning Algorithm For Deep Belief Nets”, *Neural Computation,* 18, 1527-1554, 2006.

[0152] Jouppi, et al., “In-Datacenter Performance Analysis of a Tensor Processing Unit™”, To appear at the 44th International Symposium on Computer Architecture (ISCA), Toronto, Canada, Jun. 26, 2017, pages 1-17.

[0153] LeCun, et al., “Deep Learning”, Nature, Vol. 521, 28 May 2015, pages 436-444.

[0154] Marvin, “Blockchain A-Z: Everything You Need to Know About the Game-Changing Tech Beneath Bitcoin”, https://www.pcmag.com/.../blockchain-a-z-everything-you-need-to-know-about-the-g..., June 3, 201.6, 9 pages.

[0155] Marvin, "Blockchain: The Invisible Technology That's Changing the World", http://www.pcmag.com/article/351486, Feb. 6, 2017, 32 pages.

[0156] Mougayar, *The Business Blockchain*, pages 6-9, 128-133. 2016, published by John Wiley & Sons, Hoboken, N.J.

[0157] Nakamoto, "Bitcoin—A Peer to Peer Electronic Cash System", citeseerx.ist.psu.edu./viewdoc/summary-?doi=10.1.1.22.1.9986, 2008, pages. 1-9

[0158] Ng, "What Artificial Intelligence Can and Can't I)o Right Now", Harvard Business Review, https://hbr.org/2016/11/what-artificial-intelligence-can-and-cant-do-right-now, Nov. 9, 2016, 5 pages.

[0159] O'Dowd, et al., "IBM's Open Blockchain, Making Blockchain Real for Enterprises". IBM Blockchain, April 2016, pages 1-20.

[0160] Ronan, "Deep Learning predicts Loto Numbers", Academy of Paris, Apr. 1, 2016, pages 1-4.

[0161] Smart Contract Alliance, "Smart Contracts: 12 Use Cases for Business and Beyond, A Technology, Legal & Regulatory Information, prepared by Smart Contracts Alliance—In collaboration with Deloitte, An industry initiative of the Chamber of Digital Commerce", December 2016, pages 1-53.

[0162] Turing, "Computing Machinery and Intelligence", Mind 49: 1950, pages 433-460.

[0163] Wood, "Ethereum: A Secure Decentralized Generalized Transaction Ledger", Homestead Draft, https://pdfs.semanticscholar.org/ac15ea808ef3b17ad754f91d3a.00fedc8f96b929.pdf, 2014, pages 1-32.

[0164] Wu, et al., "Google's Neural Machine Translation System: Bridging the Gap between Human and Machine Translation", arXiv:1609.08144v2 [cs.CL] 8 Oct. 2016, pages 1-23.

[0165] Yli-Huumo, et al., "Where Is Current Research on Blockchain Technology?—A Systematic Review", PLoS ONE, DOI 11(10):e0163477.doi:10.1371/journal.pone.0163477, Oct. 3, 2016, pages 1-27.

Glossary

[0166] 51% Attack: An attack on the Bitcoin network which allows the attacker to create fraudulent transactions, see Double Spend. This is possible because controlling more than 50% of the Bitcoin network's has rate means the attacker can out-compute everyone else who is mining.

A

[0167] Account: Accounts have an intrinsic balance and transaction count maintained as part of the Ethereum state. They also have some (possibly empty) EVM Code and a (possibly empty) Storage State associated with them. Though homogenous, it makes sense to distinguish between two practical types of account: those with empty associated EVM Code (thus the account balance is controlled, if at all, by some external entity) and those with non-empty associated EVM Code (thus the account represents an Autonomous Object). Each Account has a single Address that identifies it.

[0168] Address: A bitcoin address is used to receive and send transactions on the bitcoin network. It contains a string of alphanumeric characters, but can also be represented as a scannable QR code. A bitcoin address is also the public key in the pair of keys used by bitcoin holders to digitally sign transactions (see Public Key).

[0169] Address: A 160-bit code used for identifying Accounts.

[0170] Agreement Ledger: An agreement ledger is distributed ledger used by two or more parties to negotiate and reach agreement.

[0171] Airdrop: A method of distributing cryptocurrency amongst a population, first attempted with Auroracoin (auroracoin) in early 2014.

[0172] Algorithm: A process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer.

[0173] Altcoin: The collective name for cryptocurrencies offered as alternatives to bitcoin. Litecoin, Feathercoin and PPcoin are all altcoins.

[0174] AML: Anti-Money Laundering techniques are used to stop people converting illegally obtained funds, to appear as though they have been earned legally. AML mechanisms can be legal or technical in nature. Regulators frequently apply AML techniques to bitcoin exchanges.

[0175] App: An end-user-visible application hosted in the Ethereum Browser.

[0176] Application Program Interface (API): A specification used as an interface by components, often software components, to communicate with one another. May include specifications for routines, data structures, object classes, and variables.

[0177] Arbitrage: The generation of risk free profits by trading between markets which have different prices for the same asset.

[0178] ASIC: An Application Specific Integrated Circuit is a silicon chip specifically designed to do a single task. In the case of bitcoin, they are designed to process SHA-256 hashing problems to mine new bitcoins.

[0179] ASIC Miner: A piece of equipment containing an ASIC chip, configured to mine for bitcoins. They can come in the form of boards that plug into a backplane, devices with a USB connector, or standalone devices including all of the necessary software, that connect to a network via a wireless link or ethernet cable.

[0180] ASIC Mining: Out-of-the-box computer systems that you buy at electronics stores usually don't include the processing power that's necessary for the cryptocurrency mining process. As a result, many miners purchase separate computing devices set aside solely for mining. As an alternative, they can also get an Application Specific Integrated Circuit (ASIC); this is a specially-designed computer chip created to perform one specific function, and only that function—in this case, mining calculations. ASICs reduce the processing power and energy required for mining, and can help reduce the overall cost of the process in that way. Whether the ASIC—a term that refers to the specialized chip itself—is integrated into an existing computing system, or functions as a stand-alone device, the term "ASIC." is often used generically to refer to the overall system itself, and not just the chip.

[0181] Asymmetric Key Algorithm: This is the algorithm used to generate public and private keys, the unique codes that are essential to cryptocurrency transactions. In a symmetric key algorithm, both the sender and receiver have the same key: they can encrypt and exchange information privately, but since both parties have the decoding information, they can't keep information private from one another.

With an asymmetric key algorithm, both parties have access to the public key, but only the person with the private key can decode the encryption; this assures that only they can receive the funds.

[0182] Attestation Ledger: A distributed ledger providing a durable record of agreements, commitments or statements, providing evidence (attestation) that these agreements, commitments or statements were made.

[0183] Autonomous Agents: Software that makes decisions and acts on them without human intervention.

[0184] Autonomous Object: A notional object existent only within the hypothetical state of Ethereum. Has an intrinsic address and thus an associated account; the account will have non-empty associated EVM Code. Incorporated only as the Storage State of that account.

B

[0185] Base58: Base58 encodes binary data into text and is used to encode Bitcoin addresses. Created by Satoshi Nakamoto, its alphanumeric characters exclude "0". "O", "1", I" since they are hard to distinguish.

[0186] Base58Check: A variant of Base58 used to detect typing errors in bitcoin addresses.

[0187] Bear Trap: This is a manipulation of a stock or commodity by investors. Traders who "set" the bear trap do so by selling stock until it fools other investors into thinking its upward trend in value has stopped, or is dropping. Those who fall into the bear trap will often sell at that time, fearing a further drop in value. At that point, the investors who set the trap will buy at the low price and will release the trap-which is essentially a false bear market. Once the bear trap is released, the value will even out, or even climb.

[0188] BIP: An acronym for "Bitcoin Improvement Proposals" which can be submitted by anyone who wants to improve the Bitcoin network.

[0189] Bit: Name of a Bitcoin denomination equal to 100 satoshis (1 millionth of 1 BTC). In 2014 several companies including Bitpay and Coinbase, and various wallet apps adopted bit to display bitcoin amounts.

[0190] Bitcoin (uppercase): The well know cryptocurrency, based on the proof-of-work blockchain.

[0191] bitcoin (lowercase): The specific collection of technologies used by Bitcoin's ledger, a particular solution. Note that the currency is itself one of these technologies, as it provides the miners with the incentive to mine.

[0192] Bitcoin (unit of currency): 100,000,000 satoshis. A unit of the decentralized, digital currency which can be traded for goods and services. Bitcoin also functions as a reserve currency for the altcoin ecosystem.

[0193] Bitcoin 2.0: A reference word for applications of bitcoin or Blockchain technology that is more advanced or complicated than the basic payment system application proposed by the Bitcoin white paper. Examples of Bitcoin 2.0 projects include Counterparty, Ethereum, Blockstream, Swarm, Domus and Hedgy.

[0194] Bitcoin ATM: A bitcoin ATM is a physical machine that allows a customer to buy bitcoin with cash. There are many manufacturers, some of which enable users to sell bitcoin for cash. They are also sometimes called 'BTMs' or 'Bitcoin AVMS'. CoinDesk maintains a worldwide map of operational bitcoin ATM machines and a list of manufacturers.

[0195] Bitcoin Core: New name of Bitcoin QT since release of version 0.9 on Mar. 19, 2014. Not to confuse with CoreBitcoin, an Objective-C implementation published in August 2013.

[0196] Bitcoind: Original implementation of Bitcoin with a command line interface. Currently a part of BitcoinQT project. "D" stands for "daemon" per UNIX tradition to name processes running in background.

[0197] Bitcoin Days Destroyed: An estimate for the "velocity of money" with the Bitcoin network. This is used because it gives greater weight to bitcoins that have not been spent for a long time, and better represents the level of economic activity taking place with bitcoin than total transaction volume per day.

[0198] Bitcoin Investment Trust: This private, open-ended trust invests exclusively in bitcoins and uses a state-of-the-art protocol to store them safely on behalf of its shareholders. It provides a way for people to invest in bitcoin without having to purchase and safely store the digital currency themselves.

[0199] Bitcoinj: A Java implementation of a full Bitcoin node by Mike Hearn. Also includes SPV implementation among other features.

BitcoinJS:

[0200] An online library of javascript code used for Bitcoin development, particularly web wallets. bitcoinjs.org (http://bitcoinjs.org)

[0201] Bitcoin Market Potential Index (BMPI): The Bitcoin Market Potential Index (BMPI) uses a data set to rank the potential utility of bitcoin across 177 countries. It attempts to show which markets have the greatest potential for bitcoin adoption.

[0202] Bitcoin Network: The decentralized, peer-to-peer network which maintains the blockchain. This is what processes all Bitcoin transactions.

[0203] Bitcoin Price Index (BPI): The CoinDesk Bitcoin Price Index represents an average of bitcoin prices across leading global exchanges that meet criteria specified by the BPI. There is also an API for developers to use.

[0204] Bitcoin Protocol: The open source, cryptographic protocol which operates on the Bitcoin network, setting the "rules" for how the network runs.

[0205] BitcoinQT: Bitcoin QT is an open source software client used by your computer. It contains a copy of the blockchain and once installed it turns your computer into a node in the Bitcoin Network. Also acts as a "desktop wallet."

[0206] Bitcoin-ruby: A Bitcoin utilities library in Ruby by Julian Langschaedel. Used in production on Coinbase.com

[0207] Bitcoin Sentiment Index (BSI): The Bitcoin Sentiment Index is a measure of whether individuals feel the digital currency's prospects are increasing or decreasing on any given day, and is powered by data collected by Qriously.

[0208] Bitcoin Whitepaper: The bitcoin whitepaper was written by 'Satoshi Nakamoto' and posted to a Cryptography Mailing list in 2008. The paper describes the bitcoin protocol in detail, and is well worth a read. Satoshi Nakamoto followed this by releasing the bitcoin code in 2009.

[0209] Bitcoin white paper: In November 2008, a paper, authored (probably pseudonymously) by Satoshi Nakamoto, was posted on the newly created Bitcoin.org website with the title 'Bitcoin: A Peer-to-Peer Electronic Cash System'. The eight-page document described methods of using a peer-to-peer network to generate "a system for electronic transactions without relying on trust" and laid down the working principles of the cryptocurrency.

[0210] Bitcore: A Bitcoin toolkit by Bitpay written in JavaScript. More complete than Bitcoinjs.

[0211] BitPay: A payment processor for bitcoins, which works with merchants, enabling them to take bitcoins as payment.

[0212] BitStamp: An exchange for bitcoins that has been gaining in popularity. Read the latest Bitstamp news.

[0213] Block: This is a collection of transaction data, one of the fundamental elements of cryptocurrency. As transactions are made, the pertinent information for each one is collected—and when the gathered data reaches a predetermined size, it's bundled up as a block. As soon as possible after blocks are created, they're processed by investors for transaction verification; this process is known as mining.

[0214] Blockchain: The full list of blocks that have been mined since the beginning of the bitcoin cryptocurrency. The blockchain is designed so that each block contains a hash drawing on the blocks that came before it. This is designed to make it more tamperproof. To add further confusion, there is a company called Blockchain, which has a very popular blockchain explorer and bitcoin wallet.

[0215] Block Halving: [see Halving] The halving of the bitcoin reward that miners receive for mining a block. This takes place approximately every 4 years (every 210,000 block to be precise).

[0216] Block Header: Contains information about a block, such as the hash of the previous block header, its version number, the current target, a timestamp, and a nonce.

[0217] Block Height: Block height refers to the number of blocks connected together in the block chain. For example, Height 0, would be the very first block, which is also called the Genesis Block.

[0218] Blockchain.info: A web service running a Bitcoin node and displaying statistics and raw data of all the transactions and blocks. It also provides a web wallet functionality with lightweight clients for Android, iOS and OS X.

[0219] Block Reward: The reward given to a miner which has successfully hashed a transaction block. This can be a mixture of coins and transaction fees, depending on the policy used by the cryptocurrency in question, and whether all of the coins have already been successfully mined. Bitcoin currently awards 25 bitcoins for each block. The block reward halves when a certain number of blocks have been mined. In bitcoin's case, the threshold is every 210,000 blocks.

[0220] Bootstrapping: Technique for uploading the program onto a volunteer's computer or mobile device through a few simple instructions that set the rest of the program in motion.

[0221] BOT Trading: Software programs that operate on trading platforms, executing buy and sell orders with pre-programmed trading instructions.

[0222] Brain Wallet: [see Wallet] A bitcoin wallet which uses a long string of words to secure its coins. This "passphrase" can be memorized, allowing the wallet owner to spend bitcoins by simply remembering the passphrase.

[0223] Brainwallet.org: Utility based on bitcoin to craft transactions by hand, convert private keys to addresses and work with a brain wallet.

[0224] BTC: The short currency abbreviation for bitcoins.

[0225] Bubble: A bubble occurs when a market is driven upward by investors; this has happened in the dot-com and housing industries in the past decade or so. Factors such as industry popularity, speculation of potential worth, political influence, and many other things can combine to create these spikes in value. If the market is perceived to have "topped out," or investors believe it will no longer retain its overall worth, the bubble can "burst." This represents a massive sell-off by investors, which can make market value drop sharply. Depending on your perspective, some cryptocurrency markets may or may not have experienced periodic bubbles. The industry's naysayers insist the market is too volatile, and will continue to roller-coaster up and down, with no real stability in sight. Conversely, industry insiders claim these are the growing pains of a new field, and that digital currency fluctuations will smooth out over time.

[0226] Bull Trap: A bull trap is "set" by investors in a stock or commodity who will buy large amounts in order to artificially drive the value upward, or create a false bull market. Traders who are fooled by the bull trap will often buy shares at the inflated price, in the belief that the upward trend will continue and the shares they're buying will rise in value. Unfortunately, those who fell into the bull trap will often be left holding shares for which they paid too much, since once the trap is released, the market evens out, and sometimes even drops.

[0227] Buttonwood: A project founded by bitcoin enthusiast Josh Rossi, to form a public outcry bitcoin exchange in New York's Union Square. Named after the Buttonwood agreement, which formed the basis for the New York Stock Exchange in 1792.

[0228] Buy Order: A buy order is established when an investor approaches an exchange and wants to purchase cryptocurrency. These can range from very simple orders ("I want to spend x amount of dollars on Bitcoins") to complex ones that include factors such as time frame in which the order should be filled, range of price, and so forth. Most exchanges allow for these to be entered online, but some investors prefer to go over the details directly with an exchange representative. Buy orders don't necessarily guarantee your purchase; if your price is too low, for example, the offer may expire without being filled unless you make adjustments

C

[0229] Candlestick Chart: This is a popular at-a-glance type of chart that is commonly used in stock and commodity exchanges. Some charts use a dot to show where a certain stock or commodity closed on a given day; while this is valuable information, it doesn't show the range of price the commodity experienced during the trading day. With a candlestick chart, a vertical bar is used to show the scope of activity in a trading day; the upper edge of the bar will be the opening price (in a bear market), and the lower edge denotes the closing price (also in a bear market; in a bull market, the two are reversed). Lines extend out of the top and bottom of the bar, showing the highest and lowest trading prices for the commodity for that day (thus forming the "wick" of the candle). Candlestick charts are ideal for showing day-to-day market activity in a concise—but still accurate—way, denoting the full range of activity for that period.

[0230] Capital Controls: these are local measures such as transaction taxes, limits, or other prohibitions that a government can use to regulate flows from capital markets into and out of the country.

[0231] Casascius Coins: Physical collectible coins produced by Mike Caldwell. Each coin contains a private key under a tamper-evident hologram. The name "Casascius" is formed from a phrase "call a spade a spade", as a response to a name of Bitcoin itself.

[0232] Central Ledger: A central ledger refers to a ledger maintained by a central agency.

[0233] Change: Informal name for a portion of a transaction output that is returned to a sender as a "change" after spending that output. Since transaction outputs cannot be partially spent, one can spend 1 BTC out of 3 BTC output only be creating two new outputs: a "payment" output with I BTC sent to a payee address, and a "change" output with remaining 2 BTC (minus transaction fees) sent to the payer's addresses. BitcoinQT always uses new address from a key pool for a better privacy. Blockchain.info sends to a default address in the wallet. A common mistake when working with a paper wallet or a brain wallet is to make a change transaction to a different address and then accidentally delete it. E.g. when importing a private key in a temporary Bitcoin QT wallet, making a transaction and then deleting the temporary wallet.

[0234] Checkpoint: A hash of a block before which the BitcoinQT client downloads blocks without verifying digital signatures for performance reasons. A checkpoint usually refers to a very deep block (at least several days old) when it is clear to everyone that the block is accepted by the overwhelming majority of users and reorganization with not happen past that point. It also helps protecting most of the history from a 51% attack. Since checkpoints affect how the main chain is determined, they are part of the protocol and must be recognized by alternative clients (although the risk of reorganization past the checkpoint would be incredibly low).

[0235] Circle: Circle is an exchange and wallet service, offering users worldwide the chance to store, send, receive and exchange bitcoins.

[0236] Client: A software program running on a desktop or laptop computer, or mobile device. It connects to the bitcoin network and forwards transactions. It may also include a bitcoin wallet (see Node).

[0237] the Cloud: A reference to the Internet and functions it can carry out for anyone such as storage, file sending, and using apps.

[0238] Cloud-hashing/mining: A type of mining where people can pay to rent computer power from someone else in the cloud to mine bitcoin or other cryptocurrencies. This is done by selling mining contracts. Cloudhashing is also the name of a business which offers this service.

[0239] Coin: An informal term that means either **1** bitcoin, or an unspent transaction output that can be spent.

[0240] Coin Age: The age of a coin, defined as the currency amount multiplied by the holding period.

[0241] Coinbase: Another name for the input used in a bitcoin's generation transaction. When a bitcoin is mined, it doesn't come from another bitcoin user, but is generated as a reward for the miner. That reward is recorded as a transaction, but instead of another user's bitcoin address, some arbitrary data is used as the input. Coinbase is also the name of a bitcoin wallet service that also offers payment processing services for merchants and acts as an intermediary for purchasing bitcoins from exchanges.

[0242] Coinbase.com: US-based Bitcoin/USD exchange and web wallet service.

[0243] Cold Storage: The safest way to store your private keys is by keeping them offline in "cold storage". This could be in the form of a hardware wallet, USB stick or paper wallet. These wallets are known as "cold wallets".

[0244] Collective Mining: The commitment of resources and materials to the process of mining digital currency data blocks often proves to be too expensive for individuals to take part. As a result, many enterprising businesses have worked out a way to make mining more affordable for those miners who would otherwise be left out. These companies invest in the hardware that allows for high-end mining power, and they in turn lease the access to this mining capability to third parties. As an individual miner, this means you can sign a contract that allows you to use a predetermined amount of mining power through cloud computing, without the hassle or expense of buying or maintaining the processing power needed to do so. The block rewards that come with the successful mining of the data block go to the individual miner who purchased the contract from the collective mining company.

[0245] Colored Coins: A proposed add-on function for bitcoin that would enable bitcoin users to give them additional attributes. These attributes could be user-defined, enabling you to mark a bitcoin as a share of stock, or a physical asset. This would enable bitcoins to be traded as tokens for other property.

[0246] CompactSize: Original name of a variable-length integer format used in transaction and block serialization. Also known as "Satoshi's encoding". It uses 1, 3, 5 or 9 bytes to represent any 64-bit unsigned integer. Values lower than 253 are represented with 1 byte, bytes 253, 254 and 255 indicate 16-, 32- or 64-bit integer that follows. Smaller numbers can be presented different. In bitcoin-ruby it is called "var_int", in Bircoinj it is Varint. BitconQT also has even more compact representation called Varint which is not compatible with CompactSize and used in block storage.

[0247] Confirmation: The act of hashing a bitcoin transaction successfully into a transaction block, and cementing its validity. A single confirmation will take around 10 minutes, which is the average length of time for a transaction block to be hashed. However, some more sensitive or larger transactions may require multiple confirmations, meaning that more blocks must be hashed and added to the blockchain after the transaction's block has been hashed. Each time another block is added to the blockchain after the transaction's block, the transaction is confirmed again.

[0248] Confirmation Number: Confirmation number is a measure of probability that transaction could be rejected from the main chain. "Zero confirmations" means that transaction is unconfirmed (not in any block yet). One confirmation means that the transaction is included in the latest block in the main chain. Two confirmations means the transaction is included in the block right before the latest one. Probability of transaction being reversed ("double spent") is diminishing exponentially with more blocks added "on top" of it.

[0249] Confirmed Transaction: Transaction that has been included in the blockchain.

[0250] Probability of transaction being rejected is measured in a number of confirmations.

[0251] Consensus Point: A point—either in time, or defined in terms of a set number or volume of records to be added to the ledger—where peers meet to agree the state of the ledger.

[0252] Consensus Process: The process a group of peers responsible for maintaining a distributed ledger used to reach consensus on the ledger's contents.

[0253] Continuation Graph Pattern: When you take a look at a market value graph on a digital currency exchange.site, you'll be able to see at a glance the upward ("bull" market) and downward ("bear" market) trend lines. However, on occasion you'll see graph patterns that show fluctuations that go against the flow of the current trend, only for the trend to continue in the same direction afterward. This type of graph pattern is known as a "continuation" type; though there may be momentary up-and-down movement in a currency's value, from a macro view the trend hasn't really changed direction. Continuation graph patterns show that investors have tested the current trend and found it to be sound—therefore, it continues.

[0254] Contract: Informal term used to mean both a piece of EVM Code that may be associated with an Account or an Autonomous Object.

[0255] Core Developers: Programmers working on the open-source Source Code for Bitcoin. They are not formally employed by or paid by, and are not in control of, the Bitcoin Network; however, they have elevated access on the GitHub resource page for the Bitcoin Network where the main "reference" version of the Source Code is developed.

[0256] Counterfeiting: The act of imitating something in order to commit fraudulent behavior. An example of this is shopping with fake money.

[0257] CPU: Central Processing Unit—the 'brain' of a computer. In the early days, these were used to hash bitcoin transactions, but are now no longer powerful enough. They are still sometimes used to hash transactions for altcoins.

[0258] Craig Stephen Wright: The biggest mystery behind Bitcoin and blockchain is who authored the infamous 2008 white paper, the true identity behind the pseudonym Satoshi Nakamoto. Most recently, the wild goose chase has focused on an Australian coder and entrepreneur, Craig Stephen Wright, though there is still plenty of speculation as to whether Wright is the real deal or an elaborate con artist (especially since he has declined to prove it). It would seem the search for the father of the blockchain continues.

[0259] Crowdsourcing: The pooling of resources such as information or money contributed by the general population, to a goal. This is usually done online via websites where people can donate.

[0260] Cryptocurrency: A form of currency based on mathematics alone. Instead of fiat currency, which is printed, cryptocurrency is produced by solving mathematical problems based on cryptography.

[0261] Cryptography: The use of mathematics to create codes and ciphers that can be used to conceal information. Used as the basis for the mathematical problems used to verify and secure bitcoin transactions.

[0262] CSRNG: Acronym for "Cryptographically Secure Random Number Generator", used in private key generation for bitcoin wallets.

[0263] Cup and Handle: This is a pattern that appears on market value graphs when investors want to test the validity of an upward, or "bullish," trend in a commodity market. The upward trend, due to investor buying and selling, will gradually slope downward, then back up again, in a gently-sloping "Letter U" shape. After this "cup" is formed, the market will be tested again briefly, making a quick downward slope that's considerably smaller (and shorter in duration) than the "cup" preceding it: this forms the "handle" to the teacup shape. The cup and handle is considered a "continuation" pattern, in that, once the handle is formed, the upward trend will continue.

[0264] Cyberclones: Created by corporations by fracking digital world for their data.

D

[0265] DAO: An acronym for "Decentralised Autonomous Organization", a theoretical company that could exist in the cloud and carry out business according to preset algorithms, needing no human management. Also known as "DACs".

[0266] Darksend: Darksend is Darkcoin's decentralized mixing implementation, which was designed to give users of Darkcoin greater transactional privacy/anonymity.

[0267] Day Trading: This is the practice of buying and/or selling a stock or commodity, with the beginning-to-end process of the trade taking place all within the same calendar day. Day traders look for small price shifts minute-to-minute, and do their best to maximize their profits (or at least minimize their losses) by making several transactions a day-but without leaving any business unfinished overnight. Day traders depend on "micro-trends," which are minuscule shifts in market value, as compared to regular traders, who may observe the trends of a stock or commodity over several days, weeks or months before taking action.

[0268] DDoS: A distributed denial of service attack uses large numbers of computers under an attacker's control to drain the resources of a central target. They often send small amounts of network traffic across the Internet to tie up computing and bandwidth resources at the target, which prevents it from providing services to legitimate users. Bitcoin exchanges have sometimes been hit with DDoS attacks.

[0269] Dead Cat Bounce: In market trading terms, this somewhat unsavory phrase relates to a momentary recovery in a downward trend for a stock or commodity, such as cryptocurrency. When there's a bear market—that is to say, a market in which a commodity's values are steadily moving downward—there are two types of recovery. The first type is a true recovery, in which the downward slide is reversed over a long period of time, and prices trend upward consistently. The second type is the "dead cat bounce." The price trend—which has been going downward for a long period of time—shifts upward briefly, usually for no more than a week or two at most. Dead cat bounces can occur in miniature—over the space of a few hours or days—but most analysts consider this version a minor blip in the market as opposed to calling it a "true" dead cat bounce. No matter the bounce's duration, it's a false recovery, and the downward trend in valuation continues afterward. The term comes from an old—and slightly disturbing—saying, "Even a dead cat will bounce if it falls from a great height."

[0270] Decentralized: This is a term you'll hear often when cryptocurrency is being discussed. In this context, it means the currency isn't issued or controlled by a centralized authority, such as a bank or government. While this means cryptocurrency isn't directly affected by inflation or governmental regulations—which its advocates insist makes for a more level international playing field—it also means its investors carry more responsibility for its well-being. They should be aware of the risks inherent with cryptocurrency, such as value fluctuation and the lack of institutional protections against theft and fraud. There's no FDIC for digital currency—as there is in the centralized US banking system—so once it's stolen, it's gone forever.

[0271] Deepweb: The content online not indexed by search engines making it difficult to access. The majority of content on the Internet resides on the deepweb and can be accessed using a program called TOR.

[0272] Deflation: The reduction of prices in an economy over time. It happens when the supply of a good or service increases faster than the supply of money, or when the supply of money is finite, and decreases. This leads to more goods or services per unit of currency, meaning that less currency is needed to purchase them. This carries some downsides. When people expect prices to fall, it causes them to stop spending and hoard money, in the hope that their money will go further later. This can depress an economy.

[0273] Demurrage: Certain currencies penalize users for hoarding, this is done via demurrage, where a fee is charged for holding unspent coins. This fee increases as time passes.

[0274] Denial of Service [DoS]: Is a form of attack on the network. Bitcoin nodes punish certain behavior of other nodes by banning their IP addresses for 24 hours to avoid DoS. Also, some theoretical attacks like 51% attack may be used for network-wide DoS.

[0275] Depth: Depth refers to a place in the blockchain. A transaction with 6 confirmations can also be called "6 blocks deep".

[0276] Desktop Wallet: A wallet that stores the private keys on your computer, which allow the spending and management of your bitcoins.

[0277] Deterministic Wallet: A wallet based on a system of deriving multiple keys from a single starting point known as a seed. This seed is all that is needed to restore a wallet if it is lost and can allow the creation of public addresses without the knowledge of the private key.

[0278] Difficulty: This number determines how difficult it is to hash a new block. It is related to the maximum allowed number in a given numerical portion of a transaction block's hash. The lower the number, the more difficult it is to produce a hash value that fits it. Difficulty varies based on the amount of computing power used by miners on the bitcoin network. If large numbers of miners leave a network, the difficulty would decrease. Thus far, however, bitcoin's growing popularity has attracted more computing power to the network, meaning that the difficulty has increased.

[0279] Digital Certificate: Pieces of code that protect messages without the encrypt-decrypt operations but users must apply (and pay an annual fee) for individual certificates and most common e-mail services do not support them (Google, Outlook, Yahoo).

[0280] Digital Commodity: A digital commodity is a scarce, electronically transferrable, intangible, with a market value.

[0281] Digital Identity: A digital identity is an online or networked identity adopted or claimed in cyberspace by an individual, organization or electronic device.

[0282] Distributed Autonomous Enterprise [DAE]: Requires little or no traditional management or hierarchy to generate customer value and owner wealth.

[0283] Distributed Application [DAPP]: A set of smart contracts that stores data on a home-listings blockchain.

[0284] Distributed Capitalism: Lowering barriers to participation.

[0285] Distributed Ledger: Distributed ledgers are a type of database that are spread across multiple sites, countries or institutions. Records are stored one after the other in a continuous ledger. Distributed ledger data can be either "permissioned" or "unpermissioned" to control who can view it.

[0286] Double Bottom Pattern: A double bottom pattern forms on a market chart when investors buy and sell to test a downward trend in value. Buying and selling will take place, and over time this will form two distinct and almost-equal valleys on the chart's trend line. Once the second valley has formed, an upward trend will develop past the point of the peaks or tops formed during the pattern's formation. Once that happens, the market is likely to be "bullish," or upward-trending, for a while; thus the double bottom pattern is considered a "reversal" pattern, transitioning from a bear to a bull market.

[0287] Double Spending: The act of spending bitcoins twice. It happens when someone makes a transaction using bitcoins, and then makes a second purchase from someone else, using the same bitcoins. They then convince the rest of the network to confirm only one of the transactions by hashing it in a block. Double spending is not easy to do, thanks to the way that the bitcoin network operates, but it is nevertheless a risk run by those accepting zero-confirmation transactions.

[0288] Double Top Pattern: A double top pattern forms on a market chart when investors buy and sell to test an upward trend in value. Buying and selling will take place, and over time this will form two distinct and almost-equal peaks on the chart's trend line. Once the second peak has formed, an downward trend will develop past the point of the dips or valleys formed during the pattern's formation. Once that happens, the market is likely to be "bearish," or downward-trending, for a while; thus the double top pattern is considered a "reversal" pattern, transitioning from a bull to a bear market.

[0289] Dust: A transaction output that is smaller than a typically fee required to spend it [sic]. This is not a strict part of the protocol, as any amount more than zero is valid. BitcoinQT refuses to mine or relay "dust" transactions to avoid uselessly increasing the size of unspent transaction outputs (UTXO) index.

[0290] Dust Transaction: A transaction for an extremely small amount of bitcoins, which offers little financial value, but takes up space in the blockchain. The bitcoin developer team has taken efforts to eliminate dust transactions by increasing the minimum transaction amount that will be relayed by the network.

E

[0291] ECDSA: The Elliptic Curve Digital Signature Algorithm is the lightweight cryptographic algorithm used to sign transactions in the Bitcoin protocol.

[0292] Elliptic Curve Arithmetic: A set of mathematical operations defined on a group of points on a 2D elliptic curve. Bitcoin protocol uses predefined curve secp256k1. Here is the simplest possible explanation of the operations: you can add and subtract points and multiply them by an integer. Dividing by an integer is computationally infeasible (otherwise cryptographic signatures will not work). The private is a 256-bit integer and the public key is a product of a predefined point G ("generator") by that integer: A=G*a. Associativity law allows implementing interesting cryptographic schemes like Diffie-Hellman key exchange (ECDH): two parties with private keys a and b may exchange their public keys A and B to compute a shared secret point C:C+A*b=B*a because (G*a)*==(G*b)*a. The this point C can be used as a AES encryption key to protect their communication channel.

[0293] Enterprise Players: Blockchain is beginning to make serious noise in the enterprise software market, with companies such as IBM and Microsoft leveraging Ethereum in the developer environments such as Visual Studio, Microsoft Azure $14,300.00 and other cloud platforms. Internet of Things (IoT) technology, and more. Ethereum's blockchain app platform has largely been the gateway, but tech giants are now firmly in the blockchain business. The collective banking and finance industry is also embracing blockchain transactions in the form of smart contracts.

[0294] 'Entertainment': states, displays, user experience, stimuli (light, sound, tactile), Title/Value Transfer, game

[0295] Escrow: The act of holding funds or assets in a third-party account to protect them during an asynchronous transaction. If Bob wants to send money to Alice in exchange for a file, but they cannot conduct the exchange in person, then how can they trust each other to send the money and file to each other at the same time? Instead, Bob sends the money to Eve, a trusted party who holds the funds until Bob confirms that he has received the file from Alice. She then sends Alice the money.

[0296] ETF: Acronym for "Exchange Traded Fund". These are investment funds traded on stock markets that track the price index of an underlying asset.

[0297] Ethereum Browser: (aka Ethereum Reference Client) A cross-platform GUI of an interface similar to a simplified browser (a la Chrome) that is able to host sandboxed applications whose backend is purely on the Ethereum protocol.

[0298] Ethereum Runtime Environment: (aka ERE) The environment which is provided to an Autonomous Object executing in the EVM. Includes the EVM but also the structure of the world state on which the EVM relies for certain I/O instructions including CALL & CREATE.

[0299] Ethereum Virtual Machine: (aka EVM) The virtual machine that forms the key part of the execution model for an Account's associated EVM Code.

[0300] EVM Assembly: The human-readable form of EVM code.

[0301] EVM Code: The bytecode that the EVM can natively execute. Used to formally specify the meaning and ramifications of a message to an Account.

[0302] Exchange: A central resource for exchanging different forms of money and other assets. Bitcoin exchanges are typically used to exchange the cryptocurrency for other, typically fiat, currencies.

[0303] Exchange Rate: With traditional currency, this term refers to the comparative worth of one government-issued currency to another. For example, if you're an American looking to make a purchase from a merchant in England, in order to do so you'd want to take a look at the exchange rate between the US dollar and the British pound before making your purchase. This way, you'll know exactly how much you'll be spending in your currency as it applies to the other. Since cryptocurrency is international in nature, and has the same worth no matter what country you're in, the term "exchange rate" takes on a different meaning. With digital currency, it can mean one of two things: How the currency compares to a traditional currency such as the US dollar, or how it stacks up against another type of cryptocurrency (such as Bitcoin to Litecoin).

[0304] External Actor: A person or other entity able to interface to an Ethereum node, but external to the world of Ethereum. It can interact with Ethereum through depositing signed Transactions and inspecting the blockchain and associated state. Has one (or more) intrinsic Accounts.

[0305] Extra Nonce: A number placed in coinbase script and incremented by a miner each time the nonce 32-bit integer overflows. This is not the required way to continue mining when nonce overflows, one can also change the merkle tree of transactions or change a public key used for collecting a block reward.

F

[0306] Faucet: A technique used when first launching an altcoin. A set number of coins are pre-mined, and given away for free, to encourage people to take interest in the coin and begin mining it themselves.

[0307] Fee: See Transaction Fee.

[0308] Fiat Currency: A currency, conjured out of thin air, which only has value because people say it does. Constantly under close scrutiny by regulators due to its known application in money laundering and terrorist activities. Not to be confused with bitcoin.

[0309] Fill or Kill: This is a simple type of buy order made with a cryptocurrency exchange. The investor dictates how much currency they want, and at what price, and establishes a cutoff date for the order. The exchange will then do their best to fill the order according to those criteria. If the exchange hasn't found an appropriate match for the order by the cutoff date, the order is canceled and left unfilled. In other words, fill this order according to these guidelines and within this time frame. If you can't, kill it

[0310] FinCEN: The Financial Crimes Enforcement Network, an agency within the US Treasury Department. FinCEN has thus far been the main organization to impose regulations on exchanges trading in bitcoin.

[0311] Flag Pattern(s): This pattern forms on market value charts when investors want to test a current trend in a commodity's value. The buying and selling that takes place during this testing period—which generally last one to three weeks—forms fluctuations that can be bracketed by parallel diagonal lines, forming the "flag" shape. Flag patterns can occur during both upward-trending ("bear") and downward-trending ("bull") markets. Since they don't signify the current trend is going to reverse, the flag pattern is considered one of the "continuation" pattern types. Once the pattern is formed, the trend will continue moving in the direction it had been beforehand.

[0312] Fontas: This isn't so much a "what" as it is a "who." Fontas is a mysterious investor or group of investors who has been using pump and dump schemes to manipulate the value of various digital currencies. That is to say, he/she/they have been buying large amounts of currency at low prices, then they've used misleading information to get other investors to buy, falsely inflating the currency's price. At that point, Fontas sells a large chunk of their cryptocurrency investment for a sizable profit. Thus far, Fontas' focus has been on Bitcoin, but they are trying to do the same with Litecoin and Namecoin; however, investors are on to the scheme. Needless to say, Fontas is not exactly the most popular investor in the alternative currency industry. However, even savvy investors who weren't taken in by Fontas' scheme have to grudgingly admit its effectiveness.

[0313] Fork: The creation of an alternative ongoing version of the blockchain, typically because one set of miners begins hashing a different set of transaction blocks from another. It can be caused maliciously, by a group of miners gaining too much control over the network (see 51% attack), accidentally, thanks to a bug in the system, or intentionally, when a core development team decides to introduce substantial new features into a new version of a client. A fork is successful if it becomes the longest version of the blockchain, as defined by difficulty.

[0314] FPGA: A Field Programmable Gate Array is a processing chip that can be configured with custom functions after it has been fabricated. Think of it as a blank silicon slate on which instructions can be written. Because FPGAs can be produced en masse and configured after fabrication, manufacturers benefit from economies of scale, making them cheaper than ASIC chips. However, they are usually far slower.

[0315] Free Market: Aside from the tech giants accepting cryptocurrency and experimenting with the blockchain, the technology is evolving quite a bit at the hands of start-ups shaping a thriving blockchain market. There is a long list of blockchain start-ups on Angel List, and the types of businesses leveraging the technology range from financial technology (FinTech) start-ups such as SETL to MIT start-up Enigma, and companies such as Slock.it that bring blockchain technology to connected cars, homes and the sharing economy.

[0316] Freicoin: A cryptocurrency based on the inflation-free principles outlined by the economist Silvio Gessell.

[0317] Frictionless: In reference to payment systems, a system is "frictionless" when there are zero transaction costs or restraints on trading.

[0318] Full Node: A node which implements all of bitcoin protocol and does not require trusting any external service to validate transactions. It is able to download and validate the entire blockchain. All full nodes implement the same peer-to-peer messaging protocol to exchange transactions and blocks, but that is not a requirement. A full node may receive and validate data using any protocol and from any source. However, the highest security is achieved by being able to communicate as fast as possible with as many nodes as possible.

G

[0319] Gas: The fundamental network cost unit. Paid for exclusively by Ether (as of PoC-4), which is converted freely to and from Gas as required. Gas does not exist outside of the internal Ethereum computation engine; its price is set by the Transaction and miners are free to ignore Transactions whose Gas price is too low.

[0320] Genesis Block The very first block in the block chain.

[0321] Gigahashes/sec: The number of hashing attempts possible in a given second, measured in billions of hashes (thousands of Megahashes).

[0322] GPU: Graphical Processing Unit. A silicon chip specifically designed for the complex mathematical calculations needed to render millions of polygons in modern computer game graphics. They are also well suited to the cryptographic calculations needed in cryptocurrency mining.

[0323] Graph Gaps: On occasion, gaps will appear in trend lines on market value graphs. These gaps indicate a visible drop or rise in a commodity's value that hasn't necessarily happened due to trading. These can be the result of closed markets, statistical adjustments by analysts, or by strong news about the commodity. There are three types of gaps:

[0324] 1. Breakaway Gap. These appear at the beginning of a strong upward or downward trend, and represent very high-volume trading.

[0325] 2. Runaway Gap. These occur during an upward or downward trend, and represent a quick momentary intensification of that trend.

[0326] 3. Exhaustion Gap. This occurs toward the end of an upward or downward trend, and tends to indicate a small trend in the opposite direction

H

[0327] Halving: Bitcoins have a finite supply, which makes them a scarce digital commodity. The total amount of bitcoins that will ever be issued is 21 million. The number of bitcoins generated per block is decreased 50% every four years. This is called "halving." The final halving will take place in the year 2140.

[0328] Hard Fork: Some people use term hard fork to stress that changing Bitcoin protocol requires overwhelming majority to agree with it, or some noticeable part of the economy will continue with original blockchain following the old rules.

[0329] Hardware Wallet: A bitcoin wallet which stores users bitcoins offline on hardware devices

[0330] Hash: A mathematical process that takes a variable amount of data and produces a shorter, fixed-length output. A hashing function has two important characteristics. Firstly, it is mathematically difficult to work out what the original input was by looking at the output. Secondly, changing even the tiniest part of the input will produce an entirely different output.

[0331] to HASH: To compute a hash function of some data. If hash function is not mentioned explicitly, it is the one defined by the context. For instance, "to has a transaction" means to compute Hash256 of binary representation of a transaction.

[0332] Hash160: SHA-256 hashed with RIPEMD-160 it is used to produce an address because it makes a smaller hash (20 bytes vs. 32 bytes) than SHA-256, but still uses SHA-256 internally for security. BTCHash160( ) in CoreBitcoin. Hash160( ) in BitcoinQT. It is also available in scripts as OP_HASH160.

[0333] Hash, Hash256: When not speaking about arbitrary has functions, Hash refers to two rounds of SHA-256. That is, you should compute a SHA-256 hash of your data and then another SHA-256 hash of that hash. It is used in block header hashing, transaction hashing, making a merkle tree of transactions, or computing a checksum of an address. Known as BTCHash2560( ) in CoreBitcoin, Hash( ) in BitcoinQT. It is also available in scripts as OP_HASH256.

[0334] Hash Function: A hash function takes an arbitrary input such as a string of integers (a key) and outputs a value of a pre-specified length (a hash). Bitcoin uses a cryptographic hash function to secure the network.

[0335] Hash Rate: The number of hashes that can be performed by a bitcoin miner in a given period of time (usually a second).

[0336] Hash Type (hashtype): A single byte appended to a transaction signature in the transaction input which describes how the transaction should be hashed in order to verify that signature. There are three types affecting outputs: ALL (default), SINGLE, NONE and one optional modifier ANYONECANPAY affecting the inputs (can be combined with either of the first three). ALL requires all outputs to be hashed (thus, all outputs are signed). SINGLE clears all output scripts but the one with the same index as the input in question. NONE clears all outputs thus allowing changing them at will. ANYONECANPAY removes all inputs except the current one (allows anyone to contribute independently.) The actual behavior is more subtle than this overview, you should check the actual source code for more comments.

[0337] Head and Shoulders Pattern: The head and shoulders pattern forms on a market value chart when two smaller fluctuations in value bracket a larger one in the middle. There are two types of head and shoulders patterns, both of which are illustrated in the image above. One is the traditional head and shoulders, viewed "right side up" if you were looking at the bust of a human being. The fluctuations forming the head and shoulders represent investors buying and selling to test a current trend. The regular head and shoulders pattern represents a reversal from a "bull" (upward-trending) market to a "bearish" (downward-trending) one, whereas the inverted head and shoulders pattern shows the opposite, from bear to bull. Because of these characteristics, the head and shoulders pattern is listed among those of the "reversal" type.

[0338] Height: See Block Height

[0339] Hot Wallet: A bitcoin wallet that has an active connection to the Internet. These are used for "everyday" transactions and should never hold large amounts of bitcoin, since their connectivity reduces their security.

[0340] HTML: Acronym for "HyperText Markup Language", the language in which webpages are written.

[0341] HTTP: Acronym for "HyperText Transfer Protocol", this is the underlying protocol for the world wide web.

[0342] Hybrid Wallet: This is a cryptocurrency storage and maintenance system that is a combination of a software wallet (stored on your home computer) and a web wallet (stored on a third-party server). The bulk of your digital currency account information is stored on the wallet host's server—except for one important detail. Your private key (the code that uniquely identifies you) is stored only on your own device. When you make a transaction, your private key is encrypted on the way to the exchange's server, so they never know what your private key is. This is an impressive security feature, but access to your private key also includes a password that—again—only you know. If you lose or forget that password, access to your account could be denied, and you could potentially lose your account balance forever.

I

[0343] Industrial Blockchain: Secure transactional capability to watches and other wearable devices.

[0344] Inflation: When the value of money drops over time, causing prices for goods to increase. The result is a drop in purchasing power. Effects include less motivation to hoard money, and more motivation to spend it quickly while the prices of goods are still low.

[0345] Input: The part of a bitcoin transaction denoting where the bitcoin payment has come from. Typically, this will be a bitcoin address, unless the transaction is a generation transaction, meaning that the bitcoin has been freshly mined (see Coinbase).

[0346] Intellectual Property: One use case for blockchains is in securing digital assets and the intellectual property (IP) that currently sit at the mercy of the Internet. It is another area in which smart contracts come into play, particularly around digital multimedia files such as movies and music. In theory, artists, studios, and content providers believe blockchain could be the answer to piracy. This kind of IP protection could also extend to the use of copyrighted code and software, or something as trivial and commonplace as sharing Netflix passwords or grabbing an image off of Google that is not labeled for reuse.

[0347] Interface System and methods by which two or more computers talk to each other over a network, such as the Internet, using a common language that they both understand.

[0348] Issuer: We admit openly that we use this as a term of convenience when we talk about cryptocurrency. With traditional currency, the issuer would be the US Treasury for American bills and coins, for example. Technically, digital currency coins aren't issued, they're created by the mining process. There's no central bank, no government deciding when new cryptocurrency comes into being: it's "minted" when investors mine the data blocks. There's really no one owner of Bitcoin, and no corporate board making the decisions; all of its investors have a vested interest and a share in it. As such, when we use the term "issuer," we mean the investors in a type of cryptocurrency; we use it conceptually and not literally.

[0349] Jumping-off Point: The applications for blockchain are boundless. There are schools using blockchain to record and verify student credentials. Firms such as Deloitte are talking about using blockchain for tax collection. Congressional representatives have been given blockchain briefings. Even the US Postal Service (USPS) published a report on possibly adopting blockchain in its operations. Blockchain is still in its relative infancy, but a decade from now, there is no telling where you might find it.

K

[0350] Key: Could mean an ECDSA public or private key, or AES symmetric encryption key. AES is not used in the protocol itself (only to encrypt the ECDSA keys and other sensitive data), so usually the word key means an ECDSA key. When talking about keys, people usually mean private keys as public key can always be derived from a private one. See Private Key and Public Key.

[0351] Key Pool: Some wallet applications that create new private keys randomly keep a pool of unused pre-generated keys BitcoinQT keeps 100 keys by default). When a new key is needed for change address or a new payment request, the application provides the oldest key from the pool and replaces it with a fresh one. The purpose of the pool is to ensure that recently used keys are always already back up on external storage. Without a key pool you could create a new key, receive a payment on its address and then have your hard disk died before backing up this key. A key pool guarantees that this key was already backed up several days before being used. Deterministic wallets do not use a key pool because they need to back up a single secret key.

[0352] Kilohashes/sec: The number of hashing attempts possible in a given second, measured in thousands of hashes.

[0353] Kimoto Gravity Well: A mining difficult readjustment algorithm, which was created in 2013 for Megacoin, an altcoin. The well allows difficulty readjustment to occur every block, instead of every 2016 blocks for Bitcoin. This was done as a response to concern about multi pool mining schemes.

[0354] KYC: Know Your Client/Customer rules force financial institutions to vet the people they are doing business with, ensuring that they are legitimate.

L

[0355] Laundry: Also known as a "mixing service", they combine funds from various users and redistribute them, making tracing the bitcoins back to their original source very difficult by mixing their "taint".

[0356] Ledger: An append-only record store, where records are immutable and may hold more general information than financial records.

[0357] Ledger of Everything: Blockchain can address the six obstacles to a functioning Internet of Things features: resilient, robust, real-time, responsive, radically open, renewable, redactive, revenue-generating, reliable.

[0358] Leverage: In foreign currency trading, leverage multiplies the real funds in your account by a given factor, enabling you to make trades that result in significant profit. By giving leverage to a trader, the trading exchange is effectively lending them money, in the hope that it will earn back more than it loaned in commission. Leverage is also known as a margin requirement.

[0359] Liberty Reserve: A centralized digital currency payment processor based in Costa Rica. It was shut down by the US government, after it was found guilty of money laundering.

[0360] Lightweight Client: Comparing to full node, lightweight node does not store the whole blockchain and thus cannot fully verify any transaction. There are two kinds of lightweight nodes: those fully trusting an external service to determine wallet balance and validity of transactions (e.g. blockchain.info) and the apps implementing Simplified Payment Verification (SPV). SPV clients do not need to trust any particular service, but are more vulnerable to 51% attack than full nodes. See Simplified Payment Verification.

[0361] Litecoin: An altcoin based on the Scrypt proof of work. Read Litecoin news to find out more.

[0362] Liquidity: The ability to buy and sell an asset easily, with pricing that stays roughly similar between trades. A suitably large community of buyers and sellers is important for liquidity. The result of an illiquid market is price volatility, and the inability to easily determine the value of an asset.

[0363] Liquidity Swap: As a financial instrument on cryptocurrency exchanges, liquidity swaps are contracts where investors offer loans to others to trade with in exchange for a set return.

[0364] LLL: The Lisp-like Low-level Language, a human-writable language used for authoring simple contracts and general low-level language toolkit for trans-compiling to.

[0365] Lock Time (locktime): A 32-bit field in a transaction that means either a block height at which the transaction becomes valid, or a UNIX timestamp. Zero means transaction is valid in any block. A number less than 500000000 is interpreted as a block number (the limit will be hit after year 11000), otherwise a timestamp.

[0366] Lottery Defined by many states as prize, chance & consideration

M

[0367] MAC Media Access Control

[0368] Main Chain: A part of the blockchain which a node considers the most difficult (see difficulty). All nodes store all valid blocks, including orphans and recompute the total difficulty when receiving another block. If the newly arrived block or blocks do not extend existing main chain, but create another one from some previous block, it is called reorganization.

[0369] Mainnet: Main Bitcoin network and its blockchain. The term is mostly used in comparison to testnet.

[0370] Margin Call: The act of calling in a margin requirement. An exchange will issue a margin call when it feels that a trader does not have sufficient funds to cover a leveraged trading position.

[0371] Margin Trading: The trading of assets or securities bought with borrowed money. A trader usually contributes an initial amount which is then used as collateral for their debt.

[0372] Market Order: A buy or sell order which gets executed at whatever the market prices is at the time.

[0373] Market Order: An instruction given to an exchange, asking it to buy or sell an asset at the going market rate. In a bitcoin exchange, you would place a market order if you simply wanted to buy or sell bitcoins immediately, rather than holding them until a set market condition is triggered to try and make a profit.

[0374] mBTC: 1 thousandth of a bitcoin (0.001 BTC).

[0375] Megahashes/sec: The number of hashing attempts possible in a given second, measured in millions of hashes (thousands of Kilohashes).

[0376] Mempool: A technical term for a collection of unconfirmed transactions stored by a node until they either expire or get included in the main chain. When reorganization happens, transactions from orphaned blocks either become invalid (if already included in the main chain) or moved to a pool of unconfirmed transactions. By default, bitcoind nodes throw away unconfirmed transactions after 24 hours.

[0377] Merged Mining: This allows a miner to work on multiple blockchains simultaneously, contributing to the hash rate (and thus security) of both currencies being mined. E.g. Namecoin has implemented merged mining with Bitcoin.

[0378] Merkle Tree: Merkle tree is an abstract data structure that organizes a list of data items in a tree of their hashes (like in Git, Mercurial or ZFS). In Bitcoin the merkle tree issued only to organize transactions within a block (the block header contains only one hash of a tree) so that full nodes may prune fully spent transactions to save disk space. SPV clients store only block headers and validate transactions if they are provided with a list of all intermediate hashes.

[0379] Message: Data (as a set of bytes) and Value (specified as Ether) that is passed between two Accounts, either through the deterministic operation of an Autonomous Object or the cryptographically secure signature of the Transaction

[0380] Message Call: The act of passing a message from one Account to another. If the destination account is associated with non-empty EVM Code, then the VM will be started with the state of said Object and the Message acted upon. If the message sender is an Autonomous Object, then the Call passes any data returned from the VM operation.

[0381] Microtransaction: Paying a tiny amount for an asset or service, primarily online. Micro-transactions are difficult to perform under conventional payment systems, because of the heavy commissions involved. It is difficult to pay two cents to read an online article using your credit card, for example.

[0382] Miner: A computer participating in any cryptocurrency network performing proof of work. This is usually done to receive block awards.

[0383] Mining: The act of generating new bitcoins by solving cryptographic problems using computing hardware.

[0384] Mining Algorithm: The algorithm used by a cryptocurrency to sign transactions in the Bitcoin network, adding blocks onto the blockchain.

[0385] Mining Contract: A method of investing in bitcoin mining hardware, allowing anyone to rent out a pre-specified amount of hashing power, for an agreed amount of time. The mining service takes care of hardware maintenance, hosting and electricity costs, making it simpler for investors.

[0386] Mining Pool: A group of miners who have decided to combine their computing power for mining. This allows rewards to be distributed more consistently between participants in the pool.

[0387] Mint: Satoshi distributed the mint by linking the issuance of bitcoins to the creation of a new block ledger, putting the power to mint into all the hands of the peer network.

[0388] Mintage Cap: As cryptocurrency miners process blocks of transaction data, they generate new coins as a result. Cryptocurrency is a young industry, and its issuers want enough coins to go around to satisfy new investors as they join. These new coins are mathematically designed to be turned out at a stable rate, so the value of the currency will remain relatively stable, too (there will be fluctuations, as in any other commodity market, but not as wild as they would be if the commodity was extremely limited in availability). Over time, however, the mathematics of coin creation are also designed to end, to avoid over-saturation of the market and currency devaluation. In plain English, that means most cryptocurrencies will eventually stop being created when they reach a predetermined amount known as a mintage cap. Once the last coin's created, there won't be any more. In most cases, the cap won't be reached for a number of years-that's by design, so new investors will be allowed to join up for some time to come. The majority of cryptocurrencies have mintage caps set: however, a few—like Peercoin—don't.

[0389] Minting: the process of rewarding users in proof of stake coins. New coins are minted as the reward for verifying transactions in a block.

[0390] Mixing: A process of exchanging coins with other persons in order to increase privacy of one's history. Sometimes it is associated with money laundering, but strictly speaking it is orthogonal to laundering. In traditional banking, a bank protects customer's privacy by hiding transactions from all 3rd parties. In Bitcoin any merchant may do a statistical analysis of one's entire payment history and determine, for instance, how many bitcoins one owns. While it is still possible to implement KYC (Know Your customer) rules on a level of every merchant, mixing allows to be separate information about one's history between the merchants. Most important use cases for mixing are: 1) receiving a salary as a single bit monthly payment and then spending it in small transactions ("cafe sees thousands of dollars when you pay just $4"); 2) making a single payment and revealing connection of many small private spendings ("car dealer sees how much you are addicted to the coffee"). In both cases your employer, a café and a car dealer may comply with KYC/AML laws and report your identity and transferred amounts, but neither of them need to know about each other. Mixing bitcoins after receiving a salary and mixing them before making a big payment solves this privacy problem.

[0391] Mixing Service: service that mixes your bitcoins with someone else's, sending you back bitcoins with different inputs and outputs from the ones that you sent to it. A mixing service (also known as a tumbler) preserves your privacy because it stops people tracing a particular bitcoin to you. It also has the potential to be used for money laundering.

[0392] Mobile Wallet: A wallet which runs a "Mobile client", allowing people to have bitcoin wallets on their phones and tablet computers and pay on the go.

[0393] Monetary Policy: Another breakthrough is to preserve value programmed into the software.

[0394] Money Laundering: The act of trying to "clean" money earned from criminal activity by converting these profits to what appear to be legitimate assets.

[0395] M-of-N Multi-signature Transaction: A transaction that can be spent using M signatures when N public keys are required (M is less or equal to N). Multi-signature transactions that only contain one OP_CHECKMULTSIG opcode and N is 3, 2 or 1 are considered standard.

[0396] Mt. Gox: One of the first bitcoin exchanges, and at one time the most popular. Mt. Gox has since gone into administration. Based in Japan, the exchange was started by Jed McCaleb in 2010.

[0397] Multisig: Multi-signature addresses allow multiple parties to partially seed an address with a public key. When someone wants to spend some of the bitcoins, they need some of these people to sign their transaction in addition to themselves. The needed number of signatures is agreed at the start when people create the address. Services using multi-signature addresses have a much greater resistance to theft.

N

[0398] Namecoin: An altcoin designed to provide an alternative to the traditional domain name system (DNS). Users can register .bit domains, accessible via proxy servers, by paying with namecoins.

[0399] Network Effect: The increase in value of a good or service that occurs when its use becomes more widespread.

[0400] NFC: Acronym for "Near Field Communication", a low power, short range method of wireless communication. This can be used to build upon RFID systems and is what contactless smart cards (oyster cards) and payment systems (paypass) use. Most recently implement in the Apple Pay app.

[0401] Node: A computer connected to the bitcoin network using a client that relays transactions to others (see client).

[0402] Nonce: A random string of data used as an input when hashing a transaction block. A nonce is used to try and produce a digest that fits the numerical parameters set by the bitcoin difficulty. A different nonce will be used with each hashing attempt, meaning that billions of nonces are generated when attempting to hash each transaction block.

[0403] Non-standard Transaction: Any valid transaction that is not standard. Non-standard transactions are not relayed or mined by default BitcoinQT nodes (but are relayed and mined on testnet). However, if anyone puts such transaction in a block, it will be accepted by all nodes. In practice it means that unusual transactions will take more time to get included in the blockchain. If some kind of non-standard transactions becomes useful and popular, it may get named standard and adopted by users (like it). See Standard Transaction.

[0404] Noob Trap: "Noob" is an abbreviation for the term "new blood," and is also sometimes expressed as "newb" or "newbie." It applies to anyone who is a newcomer to a given community—in this case, investing in digital currency. Most alternative currency investors are good folks, and are willing to lend a helping hand and advice to those who are new to the game. However, there are also folks who see noobs as an easy mark, and these unscrupulous investors often use market manipulation methods to take advantage of those who may not yet know any better. Luckily, some judicious studying of these methods can help new investors protect themselves from falling into market manipulation traps. For better understanding of the types of noob traps there are in the digital currency world, see the terms Bear Trap, Bull Trap and Pump and Dump.

[0405] Novacoin: Though this type of cryptocurrency is not yet near the value or overall investor numbers of the big players in the industry, Novacoin still holds a spot in the top five; not bad, considering it was introduced in February 2013. Novacoin uses the Scrypt mining algorithm, and is mined by the combined proof-of-work and proof-of-stake methods.

O

[0406] Object: Synonym for Autonomous Object.

[0407] OffBlockchain Transactions: Exchanges of value which occur off the blockchain between trusted parties. These occur because they are quicker and do not block the blockchain.

[0408] Off-Ledger Currency: A currency minted off-ledger and used on-ledger. An example of this would be using distributed ledgers to manage a national currency.

[0409] Offline Storage: This concept relates to how your cryptocurrency is stored. If your currency is online—on an active drive on a computer that's turned on, or accessible through cloud computing—that means it's also accessible by other computer users. Sometimes that access takes place without your knowledge. This can lead to hacking and theft, since cryptocurrency—by design—isn't connected directly to any one person. As such, it's important to keep your unique currency information offline as often as possible; it's best to do so unless the currency is directly in use for a transaction. Two of the best ways to keep your investment info offline is to store it on an external drive that can be disconnected from your computer when it's not needed, or to print it out and store it in a paper wallet. If you decide to take advantage of a wallet service from a cryptocurrency exchange, one of the first questions you should ask them should be about offline information storage, since digital currency theft is usually untraceable and irreversible.

[0410] On-Ledger Currency: A currency minted on-ledger and used on-ledger. An example of this would be cryptocurrency. Bitcoin.

[0411] Opcode: 8-bit code of script operation. Codes from 0x01 to 0x4B (decimal 75) are interpreted as a length of data to be pushed on the stack of the interpreter (data bytes follow the opcode). Other codes are either do something interesting, or disabled and cause transaction verification to fail, or do nothing (reserved for future use). See Script.

[0412] Open Network Enterprises: As smart contracts grow in complexity and interoperate with other contracts then contribute to this.

[0413] Open Source: The practice of sharing the source code for a piece of computer software, allowing it to be distributed and altered by anyone.

[0414] Orphan Block: A block which is not a part of the valid blockchain, but which was instead part of a fork that was discarded.

[0415] OTC Exchange: An exchange in which traders make deals with each other directly, rather than relying on a central exchange to mediate between them.

[0416] Output: The destination address for a bitcoin transaction. There can be multiple outputs for a single transaction.

[0417] Owners of Coin: Ethereum chose this as its economic set. Ripple and Stellar chose the social network.

[0418] Owners of the Computing Power: Satoshi chose this economic set. This requires these miners to consume a resource external to the network, namely electricity, if they want to participate in the reward system.

P

[0419] Paper Wallet: A printed sheet containing one or more public bitcoin addresses and their corresponding private keys. Often used to store bitcoins securely, instead of using software wallets, which can be corrupted, or web wallets, which can be hacked or simply disappear. A useful form of cold bitcoin storage.

[0420] Participant: An actor who can access the ledger: read records or add records to.

[0421] Pay-to-Script Hash: A type of script and address that allows sending bitcoins to arbitrary complex scripts using a compact hash of that script. This allows payer to pay much smaller transaction fees and not wait very long for a non-standard transaction to get included in the blockchain. Then the actual script matching the hash must be provided by the payee when redeeming the funds. P2SH addresses are encoded in Base58 Check just like regular public keys and start with number "3".

[0422] Peer: An actor that shares responsibility for maintaining the identity and integrity of the ledger.

[0423] Peercoin: The first cryptocurrency to implement "Proof of Stake" alongside Proof of Work.

[0424] P2P: Peer-to-peer. Decentralized interactions that happen between at least two parties in a highly interconnected network. An alternative system to a 'hub-and-spoke' arrangement, in which all participants in a transaction deal with each other through a single mediation point.

[0425] Pennant Pattern: This pattern forms on market value charts when investors want to test a current trend in a commodity's value. The buying and selling that takes place during this testing period—which generally last one to three weeks—forms fluctuations that can be bracketed by converging diagonal lines, forming a "pennant" shape. These pennant patterns can occur during both upward-trending ("bear") and downward-trending ("bull") markets. Since they don't signify the current trend is going to reverse, the pennant pattern is considered one of the "continuation" pattern types. Once the pattern is formed, the trend will continue moving in the direction it had been beforehand.

[0426] Permissioned Ledger: A permissioned ledger is a ledger where actors must have permission to access the ledger. Permissioned ledgers may have one or many owners, when a new record is added, the ledger's integrity is checked by a limited consensus process. This is carried out by trusted actors—government departments or banks, for example—which makes maintaining a shared record much simpler that the consensus process used by unpermissioned ledgers. Permissioned block chains provide high-verifiable data sets because the consensus process creates a digital signature, which can be seen by all parties. A permissioned ledger is usually faster than an unpermissioned ledger.

[0427] Phone-to-Phone Transfer: This is a mobile application feature that allows the instantaneous transfer of information from one smartphone to another. If two mobile device users want to exchange data, and both have this feature installed and activated on their phones, they can make the transfer simply by having their devices in close proximity to each other. These are also sometimes called "touch transfers."

[0428] Platform Exchange: This is a digital currency exchange that limits the role they play in transactions made between investors. The majority of exchanges are there to facilitate these transactions, and make them easier to carry out. The exchange will sort through buy and sell orders, and will then match up investors who meet the criteria of the order in question. Their algorithms are designed so the trades being made are both secure and fair to both parties involved. Beyond that, however, the exchange does not play any "middleman" or mediating role. This is in contrast to exchanges that will hold the transaction funds in escrow, or will discuss the details of the trade with both investors before moving forward.

[0429] Pool: A collection of mining clients which collectively mine a block, and then split the reward between them. Mining pools are a useful way to increase your probability of successfully mining a block as the difficulty rises.

[0430] PPCoin: AKA Peercoin or P2P coin. An altcoin using the proof of stake mechanism in conjunction with proof of work. Based on a paper produced by Sunny King and Scott Nadal.

[0431] Pre-mining: The mining of coins by a cryptocurrency's founder before that coin has been announced and details released to others who may wish to mine the coin. Pre-mining is a common technique used with scamcoins, although not all pre-mined coins are scamcoins (see Scamcoin).

[0432] Price Bubble: An economic cycle in which the price of a security or asset will surge unsustainably, and then crash as a selloff occurs. This is usually caused y speculation, and has been observable in bitcoin's past prices. When done deliberately, this is known as a "Pump and Dump".

[0433] Primecoin: Developed by Sunny King, Primecoin uses a proof of work system to calculate prime numbers.

[0434] Private Currency: A currency issued by a private individual or firm, typically secured against uninsured assets.

[0435] Private Key (PrivKey): An alphanumeric string kept secret by the user, and designed to sign a digital communication when hashed with a public key. In the case of bitcoin, this string is a private key designed to work with a public key. The public key is a bitcoin address (see Bitcoin Address).

[0436] Process Node: The size of a transistor in nanometers, produced during a chip fabrication process. Smaller process nodes are more efficient.

[0437] Proof of Activity: Combines proof of work and proof of stake.

[0438] Proof of Burn: This is a method of "burning" one Proof of Work cryptocurrency in order to receive a different cryptocurrency. This is a form of "bootstrapping" one cryptocurrency off another, and is done by sending coins to a verifiable unspendable address.

[0439] Proof of Capacity: Requires miners to allot a sizeable volume of their hard drive to mining.

[0440] Proof of Existence: A service provided through the blockchain that allows anyone to anonymously and securely store a proof of existence for any document they choose online. This allows people to prove that a document existed at a certain point in time and demonstrate their ownership of it, without fear of that proof being taken from them.

[0441] Proof of Stake: An alternative to proof of work, in which your existing stake in a currency (the amount of that currency that you hold) is used to calculate the amount of that currency that you can mine.

[0442] Proof of Storage: Requires miners to allocate and share disk space in distributed cloud.

[0443] Proof of Work: A system that ties mining capability to computational power. Blocks must be hashed, which is in itself an easy computational process, but an additional variable is added to the hashing process to make it more difficult. When a block is successfully hashed, the hashing must have taken some time and computational effort. Thus, a hashed block is considered proof of work.

[0444] Prosumers: Customers who produce.

[0445] Protocol Evolution: Blockchain is the result of the natural evolution of internet protocols. Wired explains the story of how the original 1974 TCP/IP internet network protocol and Tim Berner-Lee's Hyper Text Transfer Protocol (HTTP) evolved in the same way as blockchain is evolving for the next generation of the Internet, bundling multiple protocols together to form the foundation of future frameworks and "watching the birth of the internet all over again".

[0446] PSP: Payment Service Provider. The PSP offers payment processing services for merchants who wish to accept payments online.

[0447] P2SH: See Pay-to-Script Hash.

[0448] Public Key (Pubkey): An alphanumeric string which is publicly known, and which is hashed with another, privately held string to sign a digital communication. In the case of bitcoin, the public key is a bitcoin address.

[0449] Pump and Dump Inflating the value of a financial asset that has been produced or acquired cheaply, using aggressive publicity and often misleading statements. The publicity causes others to acquire the asset, forcing up its value. When the value is high enough, the perpetrator sells their assets, cashing in and flooding the market, which causes the value to crash.

Q

[0450] Quandry: Blockchain has been beset by controversy from the get-go, from the ongoing saga of Satoshi Nakamoto to the technology's inextricable link with Bitcoin and all the legality that goes with it. Blockchain enables the untraceable nature of illegal cryptocurrency transactions and has even been used to cloak infamous ransomware scams such as CryptoLocker. As the technology is adopted in more industries and use cases, the questions of accountability and ramifications need to be addressed. Already starting to see these kinds of efforts. Blockchain Alliance, a non-profit organization founded by Bitcoin advocacy groups to serve as a "public-private forum to help combat criminal activity on the blockchain." Members include major cryptocurrency players such as CoinBase, the MIT Media Lab's Digital Currency Initiative, and the Blockchain organization itself.

[0451] Quantitative Easing: A form of monetary policy where a Central

[0452] QR Code: A two-dimensional graphical block containing a monochromatic pattern representing a sequence of data. QR codes are designed to be scanned by cameras, including those found in mobile phones, and are frequently used to encode bitcoin addresses.

R

[0453] Reference Implementation: Bitcoin QT (or bitcoind) is the most used full node implementation, so it is considered a reference for other implementations. If an alternative implementation is not compatible with BitcoinQT it may be foreked, that is it will not see the same main chain as the rest of the network running BitcoinQT.

[0454] Relaying Transactions: Connected Bitcoin nodes relay new transactions between each other on best effort basis in order to send them to the mining nodes. Some transactions may not be relayed by all nodes. E.g. non-standard transactions, or transactions without a minimum fee. Bitcoin message protocol is not the only way to send the transaction. One may also send it directly to a miner, mine it yourself, or send it directly to the payee and make them to relay or mine it.

[0455] Remittance: A sum of money being sent, usually internationally, as a payment or gift.

[0456] Reorg, Reorganization: An event in the node when one or more blocks in the main chain become orphaned. Usually, newly received blocks are extending existing main chain. Sometimes (4-6 times a week) a couple of blocks of the same height are produced almost simultaneously and for a short period of time some nodes may see one block as a tip of the main chain which will be eventually replaced by a more difficult blocks(s). Each transaction in the orphaned blocks either becomes invalid (if already included in the main chain block) or becomes unconfirmed and moved to the mempool. In case of a major bug or a 51% attack, reorganization may involve reorganizing more than one block.

[0457] Replicated Ledger: A ledger with one master (authoritative) copy of the data, and many slave (non-authoritative) copies.

[0458] Reversal Graph Pattern: This is a type of pattern that forms on market value charts you'll see on many digital currency exchange websites. A reversal pattern indicates that a market that has been trending upward (known as a "bull" market) will reverse direction and start moving in a downward direction, or become a "bear" market—or vice versa. When a reversal graph pattern appears, it shows that investors have been testing the current trend, and for one reason or another they don't find it viable or sustainable—thus the market changes direction.

[0459] Reward: Amount of newly generated bitcoins that a miner may claim in a new block. The first transaction in the block allows miner to claim currently allowed reward as well as transaction fees from all transactions fees from all transactions in the block. Reward is halved ever 210000 blocks approximately every 4 years. As of Jul. 27, 2014 the reward is 25 BTC (the first halving occurred in December 2012). For security reasons, rewards cannot be spent before 100 blocks built on top of the current book.

[0460] Ripple: A payment network that can be used to transfer any currency (including ad hoc currencies that have been created by users). The network consists of payment nodes and gateways operated by authorities. Payments are made using a series of IOUs, and the network is based on trust relationships.

[0461] Rounding Bottom: Occasionally referred to as a "saucer bottom," this is a term for a pattern you may see on market value charts on exchange websites. The rounding bottom pattern is considered a "reversal" pattern; that is to say, it represents the transition over time of a downward-trending, or "bear" market, into an upward-moving "bull" market. The gently downward-sloping line on the left of the illustration above tracks the market as it eventually finds its bottom, or lowest market value, then—usually just as gently and slowly—the trend heads upward. This is a very long-term pattern, often taking several months to a couple of years to fully form.

S

[0462] Satoshi: The smallest subdivision of a bitcoin currently available (0.00000001 BTC).

[0463] Satoshi Nakamoto: The name used by the original inventor of the Bitcoin protocol, who withdrew from the project at the end of 2010.

[0464] Scamcoin: An altcoin produced with the sole purpose of making money for the originator. Scamcoins frequently use pump and dump techniques and pre-mining together.

[0465] Script: A compact turing-incomplete programming language used in transaction inputs and outputs. Scripts are interpreted by a Forth-like stack machine: each operation manipulates data on the stack. Most scripts follow the standard pattern and verify the digital signature provided in the transaction input against a public key provided in the previous transaction's output. Both signatures and public keys are provided using scripts. Scripts may contain complex conditions, but can never change amounts being transferred. Amount is stored in a separate field in a transaction output.

[0466] scriptPubKey: Original name in bitcoind for a transaction output script. Typically, output scripts contain public keys (or their hashes: see Address) that allow only owner of a corresponding private key to redeem the bitcoins in the output.

[0467] scriptSig: Original name in bitcond for a transaction input script. Typically, input scripts contain signatures to prove ownership of bitcoins sent by a previous transaction.

[0468] Scrypt: An alternative proof of work system to SHA-256, designed to be particularly friendly to CPU and GPU miners, while offering little advantage to ASIC miners.

[0469] Secret Key: Either the Private Key or an encryption key is used in encrypted wallets. Bitcoin protocol does not use encryption anywhere, so secret key typically means a private key used for signing transactions.

[0470] Sequence: A 32-bit unsigned integer in a transaction input used to replace older version of a transaction by a newer one. Only used when locktime is not zero. Transaction is not considered valid until the sequence number is 0xFFFFFFFF.

[0471] Seed: The private key used in a "deterministic wallet".

[0472] Self-Executing Contract: Also known as "smart contracts" these are protocols that facilitate or enforce the obligations of contract without the need for human intervention.

[0473] Sell Order: This takes place when an investor approaches an exchange with the intent to sell some or all of their cryptocurrency investment. Sometimes sell orders are simple and straight to the point ("Just sell what I have at the best price you can find"), or the investor can set criteria that have to be met before the sale can be made. This can include, price, time frame, percentage of holdings being sold, and so forth. Most exchanges have sell order forms that can be filled out, but if investors have specific questions or concerns, they can talk directly to an exchange representative before activating their order.

[0474] SEPA: The Single European Payments Area. A payment integration agreement within the European Union, designed to make it easier to transfer funds between different banks and nations in euros.

[0475] SHA-256: The cryptographic function used as the basis for bitcoin's proof of work system.

[0476] Sidechain: These are theoretical, independent blockchains which are "two way pegged" to the Bitcoin blockchain. These can have their own unique features and can have bitcoins sent to and from them.

[0477] Signature: A digital digest produced by hashing private and public keys together to prove that a bitcoin transaction came from a particular address.

[0478] Silk Road: An underground online marketplace, generally used for illicit purchases, often with cryptocurrencies such as bitcoin. Silk Road was shut down in early October 2013 by the FBI after owner Ross Ulbricht was arrested. Ulbricht was later convicted on money laundering and drug distribution charges.

[0479] Simplified Payment Verification (SPV): A scheme to validate transactions without storing the whole blockchain (only block headers) and without trusting any external service. Every transaction must be present with all its parent and sibling hashes in a merkle tree up to the root. SPV client trusts the most difficult chain of block headers and can validate if the transaction indeed belongs to a certain block header. Since SPV does not validate all transactions, a 51% attack may not only cause a double spend (like with full nodes), but also make a completely invalid payment with bitcoins created from nowhere. However, this kind of attack is very costly and probably more expensive than a product in question. Bitcoinj library implements SPV functionally. (See SPV)

[0480] SliceFeeds: SliceFeeds is Coin Pursuit's free social network that eliminates hassle by concentrating all traders, miners and enthusiasts contacts and cryptocurrency information in one place. Members can Slice conversations, notes, rumors, tips, links and videos to fellow community members to follow. Its network is divided into three easy-to-use sections: the network page shows statistics at a glance; the Slices page displays updates as they happen; and the profile page allows members to customize their own personal network-within-the-network. Members will also be able to monetize their unique contributions to the community; for example, bloggers can offer subscriptions (payable in digital currency, of course) for access to their exclusive content, and merchants will be able to advertise their companies and products through SliceFeeds, as well.

[0481] Slices: Slices are member-contributed content provided by members on SliceFeeds, a social media network provided by Coin Pursuit. These Slices can consist of conversations, notes, rumors, tips, links and videos for fellow community members to follow, rate and view.

[0482] Smart Contracts: Smart contracts are contracts whose terms are recorded in a computer language instead of a legal language. Smart contracts can be automatically executed by a computing system, such as a suitable distributed ledger system.

[0483] Soft Fork: Sometimes the soft fork refers to an important change of software behavior that is not a hard fork (e.g. changing mining fee policy). See Hard Fork and Fork.

[0484] Source Code: The open-source software which includes protocols governing rules for movement and ownership of bitcoins and the cryptography system that secures and verifies Bitcoin transactions.

[0485] Speculator: An individual who speculates on the price of bitcoin or any other form of asset. Aiming to make profits by buying and selling at different prices.

[0486] SPAM: Incorrect peer-to-peer messages (like sending invalid transactions) may be considered a denial of service attack. Valid transactions sending very tiny amounts and/or having low mining fees are called Dust by some people. The protocol itself does not define which transactions are not worth relaying or mining. It is a decision of every individual node. Any valid transaction in the blockchain must be accepted by the node if it wishes to accept the remaining blocks, so transaction censorship only means increased confirmation delays. Individual payees may also blacklist certain addresses (refuse to accept payments from some addresses), but that is too easy to work around using mixing.

[0487] Spent Output: A transaction output can be spent only once: when another valid transaction makes a reference to this output from its own input. When another transaction attempts to spend the same output, it will be rejected by the nodes already seeing the first transaction. Blockchain as a proof-of-work scheme allows every node to agree on which transaction was indeed the first one. The whole transaction is considered spent when all its outputs are spent.

[0488] Split: A split of a blockchain. See Fork.

[0489] SPV: Simplified Payment Verification. A feature of the Bitcoin protocol that enables nodes to verify payments without downloading the full blockchain. Instead, they need only download block headers.

[0490] Stale: When a bitcoin block is successfully hashed, any others attempting to hash it may as well stop, because it is now 'stale'. They would simply be repeating work that someone else has already done, for no reward. The tern is also used in mining pools to describe a share of a hashing job that has already been completed.

[0491] Stale Block: A block that has already been solved and thus cannot offer miners any reward for further work on it.

[0492] Standard Transaction: Some transactions are considered standard, meaning they are relayed and mined by most nodes. More complex transactions could be buggy or cause DoS attacks on the network, so they are considered non-standard and not relayed or mined by most nodes. Both standard and non-standard transactions are valid and once included in the blockchain, will be recognized by all nodes. Standard transactions are: 1) sending to a public key, 2) sending to an address, 3) sending to a P2SH address, 4) sending to a M-of-N multi-signature transaction where N is 3 or less.

[0493] Stop-Loss Order: This is a standing "get me out of here!" sell order that investors in stocks or commodities (such as cryptocurrency) use to, well . . . stop their losses. Or at least minimize them. Investors often establish a stop-loss order the minute they make a purchase. This is a sell order that specifies the price at which the currency should be sold. For example, if you buy shares of something at $100 each, you might decide to issue a stop-loss order at $60. As long as the share price remains above that number, all is well—and nothing will happen unless you contact the exchange personally. However, the second the price hits $60, all or part of your currency (whichever you specify) will be sold at your stop-loss order price. Different exchanges treat this differently; some sell immediately, and some wait to see if it's just a momentary "hiccup" on the market; if the price falls below your stop-loss limit, you'll get the latter amount for your shares.

[0494] Storage State: The information particular to a given Account that is maintained between the times that the Account's associated EVM Code runs.

T

[0495] Taint: An analysis of how closely related two addresses are when they have both held a particular bitcoin. A taint analysis could be used to determine how many steps it took for bitcoins to move from an address known for stolen coins, to the current address.

[0496] Target: A 256-bit number that puts an upper limit for a block header hash to be valid. The lower the target is, the higher the difficult to find a valid has. The maximum (easiest) target is 0x00000000FFFF0000000000000000000000000000000000000000000000000000. The difficulty and the target are adjusted every 2016 blocks (approx. 2 weeks) to keep interval between the blocks close to 10 minutes.

[0497] TCP/IP: Acronyms stand for "Transmission Control Protocol"/"Internet Protocol" and is the connection protocol used by the Internet.

[0498] Terahashes/sec: The number of hashing attempts possible in a given second, measured in trillions of hashes (thousands of Gigahashes).

[0499] Testnet: An alternative bitcoin blockchain, used purely for testing purposes.

[0500] Testnet3: The latest version of testnet with another genesis block.

[0501] Timestamp: A proof that a piece of data existed at a certain point in time. For Bitcoin this is the cryptographic proof of when transactions have taken place.

[0502] Tokenless Ledger: A tokenless ledger refers to a distributed ledger that doesn't require a native currency to operate.

[0503] TOR: An anonymous routing protocol, used by people wanting to hide their identity online.

[0504] Total Coin Supply: For many cryptocurrencies, there is a limit on the total number of coins that will ever come into existence, bitcoin's total supply is capped at 21 million coins.

[0505] Trading Walls: Generally speaking, the trend line on a chart (such as those offered by digital currency exchanges) will move more or less diagonally as trades are made. However, once in a while there is a buy or sell order that comes in which will make the trend line move directly up and down, creating a vertical line that resembles a wall. These "walls" represent a temporary high demand in interest, either in buying or selling a certain type of digital currency. If a wall is created by a large buy order, it's called a "buy wall," and if it represents a sizable sell order, it's called a "sell wall." Generically speaking, these walls are called "trading walls" or "bid walls." Once the orders have been filled—or are ignored by the market in general—the wall disappears, and the diagonal trend line continues.

[0506] Transaction: A piece of data, signed by an External Actor. It represents either a Message or a new Autonomous Object. Transactions are recorded into each block of the blockchain.

[0507] Transaction Block: A collection of transactions on the bitcoin network, gathered into a block that can then be hashed and added to the blockchain.

[0508] Transaction Database: From a purely technological perspective, blockchains are transaction databases. The hashes, keys and nodes all make up a distributed database that eschews centralized storage.

[0509] Transaction Fee: A small fee imposed on some transactions sent across the bitcoin network. The transaction fee is awarded to the miner that successfully hashes the block containing the relevant transaction.

[0510] Transaction Input: A part of a transaction that contains a reference to a previous transaction's output and a script that can prove ownership of that output. The script usually contains a signature and thus called scriptSig. Inputs spend previous outputs completely. So if one needs to pay only a portion of some previous output, the transaction should include extra change output that sends the remaining portion back to its owner (on the same or different address). Coinbase transactions contain only one input with a zeroed reference to a previous transaction and an arbitrary data in place of script.

[0511] Transaction Output: An output contains an amount to be sent and a script that allows further spending. The script typically contains a public key (or an address, a hash of a public key) and a signature verification opcode. Only an owner of a corresponding private key is able to create another transaction that sends that amount further to someone else. In every transaction, the sum of output amounts must be equal or less than a sum of all input amounts. See Change.

[0512] Triangle Pattern: Generally speaking, triangle patterns form on market value charts when investors buy and sell to test a current trend. The highs and lows of these fluctuations can be bracketed by straight lines that define the highs and lows during that testing period; these lines form an open-ended triangular shape. There are three types of triangle patterns:

[0513] 1. Descending Triangle. This is formed when the lower line of the triangle is a horizontal line, and the upper line tilts downward from left to right. The descending triangle represents a downward-trending, or "bear," market.

[0514] 2. Ascending Triangle. This is the inverse of the descending triangle, with an upward left-to-right tilted line at the bottom, and a horizontal line at the top. Ascending triangle patterns indicate an upcoming "bull," or upward-trending, market.

[0515] 3. Symmetrical Triangle. The symmetrical triangle stands out because both lines forming the triangle are tilted. It's also a more tricky pattern to predict, because it can continue in either an upward ("bullish") or downward ("bearish") direction.

[0516] Triple Bottom Pattern: A triple bottom pattern forms on a market chart when investors buy and sell to test a downward trend in value. Buying and selling will take place, and over time this will form three distinct and almost-equal valleys on the chart's trend line. Once the third valley has formed, an upward trend will develop past the point of the peaks or tops formed during the pattern's formation. Once that happens, the market is likely to be "bullish," or upward-trending, for a while; thus the triple bottom pattern is considered a "reversal" pattern, transitioning from a bear to a bull market

[0517] Triple Top Pattern: A triple top pattern forms on a market chart when investors buy and sell to test an upward trend in value. Buying and selling will take place, and over time this will form three distinct and almost-equal peaks on the chart's trend line. Once the third peak has formed, an downward trend will develop past the point of the dips or valleys formed during the pattern's formation. Once that happens, the market is likely to be "bearish," or downward-trending, for a while; thus the triple top pattern is considered a "reversal" pattern, transitioning from a bull to a bear market.

[0518] TX: see Transaction

[0519] Txin: see Transaction Input.

[0520] Txout: see Transaction Output.

U

[0521] Ubiquity: Blockchains are everywhere; at this point in the alphabet that is not news. The open-source code, universally applicable architecture of blockchains, and their ability to distribute, anonymize, protect, and keep a perfectly accurate record of web transactions makes the technology a given.

[0522] Ubtc: One microbitcoin (0.000001 BTC).

[0523] Unconfirmed Transaction: Transaction that is not included in any block. Also known as "0-confirmation" transaction. Unconfirmed transactions are relayed by the nodes and stay in the mempools. Unconfirmed transaction stays in the pool until the node decides to throw it away, finds it in the blockchain, or includes it in the blockchain, or includes it in the blockchain itself (if it is a miner). See Confirmation Number.

[0524] Unique Node List: Other blockchains such as Ripple and Stellar rely on social networks for consensus and may recommend new participants (i.e., new nodes) to generate unique mode list.

[0525] Unpermissioned Ledgers: Unpermissioned ledgers such as Bitcoin have no single owner—indeed, they cannot be owned. The purpose of an unpermissioned ledger is to allow anyone to contribute data to the ledger and for everyone in possession of the ledger to have identical copies. This creates resistance which means that no actor can prevent a transaction from being added to the ledger. Participants maintain the integrity of the ledger by reaching a consensus about its state.

[0526] UTXO Set: A collection of Unspent Transaction Outputs. Typically used in discussions on optimizing an ever-growing index of transaction outputs that are not yet spent. The index is important to efficiently validate newly created transactions. Even if the rate of the new transactions remains constant, the time required to locate and verify unspent output grows. Possible technical solutions include more efficient indexing algorithms and a more performant hardware. BitcoinQT, for example, keeps only an index of outputs matching user's keys and scans the entire blockchain when validating other transactions. A developer of one web wallet service mentioned that they maintain the entire index of UTXO and its size was around 100 Gb when the blockchain itself was only Gb. Some people seek social methods to solve the problem. For instance, by refusing to relay or mine transactions that are considered dust (containing outputs smaller than a transaction fee required to mine/relay them).

V

[0527] Vanity Address: A bitcoin address with a desirable pattern, such as a name.

[0528] Varint: This term may cause confusion as it means different formats in different Bitcoin implementations. See CompactSize.

[0529] Velocity of Money: The velocity of money is an indicator of how quickly money received is then spent again. For bitcoin, we use "bitcoin days destroyed" to measure its velocity, this can indicate whether people are hoarding or spending their bitcoins.

[0530] Venture Capitalist: Can refer to an individual or organization that provide initial funding for start-up business ventures that cannot access public funding. This money is known as "seed funding", and is usually exchanged for equity in the start-up.

[0531] Verification: Blockchains would not work as ledgers without verification. Much of this falls on miners, whose block creation software verifies hashes of transactions when bundling them into blocks. In cryptocurrency and banking scenarios, payment verification is also paramount. This verification happens through node communication in the distributed network, cross-checking a Bitcoin transaction against each node's blockchain data before sending it through.

[0532] Virgin Bitcoin: Bitcoins purchased as a reward for mining a block. These have not yet been spent anywhere.

[0533] Volatility: The measurement of price movements over time for a traded financial asset (including bitcoin).

W

[0534] Wallet: A method of storing bitcoins for later use. A wallet holds the private keys associated with bitcoin addresses. The blockchain is the record of the bitcoin amounts associated with those addresses.

[0535] Wallet: Just like a bill-and-coin wallet, this is a place to keep your digital currency. There are four types of cryptocurrency wallets:

[0536] 1. Software Wallet. These are programs you load onto your desktop or laptop computer.

[0537] 2. Mobile Wallet: These come in the form of applications you install on your smartphone or tablet computer. They usually include QR code scanning and phone-to-phone transfers for on-the-go transactions.

[0538] 3. Web Wallet: These are usually gotten through exchanges, and stored on third-party servers via cloud computing. They can be accessed by any computing device.

[0539] 4.Paper Wallet: Your digital currency can be printed out—usually in the form of OR codes—and these hard-copy cryptocurrency “bills” can be kept in a physical wallet just like traditional money.

[0540] Watchdogs: How quickly blockchains develop and see adoption in major world markets will largely fall on government oversight and regulation. The European Union’s (EU) markets watchdog—the European Securities and Markets Authority (ESMA)—recently announced it is going to take a closer look at blockchain technology. The EU watchdog is a prime example of world-governing bodies conducting a careful examination of the financial and technological risks associated with distributed ledgers. The EU won’t be the last government to take a long, hard look at blockchains before giving the green light for the sanctioned use.

[0541] Wedge Pattern: These are a type of “continuation” pattern you’ll see on market value graphs; that means they represent a momentary shift against the current trend, but the trend tends to continue in the direction it was going once the pattern is fully formed. Wedge patterns can be spotted by two diagonal, but non-converging, lines that bracket the up-and-down fluctuations that occur while investors test the current trend. There are three types of wedge patterns:

[0542] 1. Rising Wedge. This wedge shape is tilted upward; thus the name. However, a rising wedge occurs during a downward trend, or “bear” market. It’s a momentary upward shift, but the bear market continued afterward.

[0543] 2. Falling Wedge. The falling wedge is tilted downward. It represents just the opposite of the rising wedge, in that it denotes a brief downward movement during a “bull” market, which continues once the wedge is formed.

[0544] 3. Level Wedge. These appear to move in more or less a horizontal direction on a graph. Just like the rising and falling wedges, the level wedge shows a brief respite in a trend, which will continue once the wedge pattern is complete.

[0545] Wire Transfer: Electronically transferring money from one person to another. Commonly used to send and retrieve fiat currency from bitcoin exchanges.

X

[0546] XBT: Informal currency code for 1 Bitcoin (defined as 100 000 000 Satoshis). Some people proposed using it for 0.01 Bitcoin to avoid confusion with BTC. There were rumors that Bloomberg tests XBT as a ticker for 1 Bitcoin, but currently there is only ticker XBTFUND for SecondMarket’s Bitcoin Investment Trust. See BTC.

[0547] XRP: Also known as Ripple, XRP is a global payments network built on blockchain that is marketed at international banks. XRP itself is the native currency organizations can use to represent flat currency, cryptocurrency, commodities, or any other unit of value. Ripple is one of the oldest examples of open payment protocols using blockchain, but there is a laundry list of companies with different APIs, platforms and distributed payments networks. Deloitte’s Banking Industry Outlook recently released a report estimating that blockchain-based payment systems could equal the volume of the United States’ Automated Clearing House (ACH) financial transactions network by 2020.

Y

[0548] Yield Curve: Yield curves are a financial method of plotting interest rates of differing maturity. For the purposes of blockchain . . . talking about yield curves because there are more and more banks and financial firms, payments providers, and countries looking at and adopting blockchain. Companies around the world . . . are all pushing blockchain for money transfer and payments. Plus, lawmakers in the Philippines have been pushing for years to create an “e-peso” as an official electronic tender. Blockchain is taking hold in many corners of the world, but will see a wide curve of maturity in how quickly and completely the implementations see approval and adoption.

Z

[0549] Zerocoin: A protocol designed to make cryptocurrency transactions truly anonymous.

[0550] Zero-confirmation Transaction A transaction in which the merchant is happy to provide a product or service before the bitcoin’s transmission has been confirmed by a miner and added to the blockchain. It can carry a risk of double spending.

[0551] Zero-confirmation Transaction: The processing of data for cryptocurrency transactions can take anywhere from half a minute upward to over ten minutes in some cases. Though this is necessary in order to validate transactions—and guards against fraudulent activity such as double spending—the waiting period can be inconvenient for those involved in the transactions. As a result, some exchanges and businesses that deal with digital currency are offering “zero confirmation” transactions, which are almost immediately verified without waiting for the mining process to confirm the data block. Double spending—the practice in which a coin holder applies the same currency to two different transactions—is a concern with zero confirmation transactions. Since cryptocurrency is not “attached” to the person spending it in any way, by the time their double spending is discovered through the mining process, they are long gone and untraceable. With the demand for zero confirmation transactions on the upswing, entrepreneurs in the cryptocurrency industry are looking at ways to instantly verify—or deny—transactions without having to wait for mining to take place. In the meantime, many businesses levy fees to offset the financial risk of zero confirmation transactions, and yet others are refusing to accept them until the technology catches up.

[0552] Z System: IBM is openly committed to advancing blockchain technology on many fronts, but the company has even gone as far as offering a Blockchain-as-a-Service (BaaS) platform for developers on the IBM Cloud, and integrating blockchain-based apps (created through the Hyperledger Project) on IBM z Systems. IBM even plans to leverage blockchains combined with Watson on the Watson IoT platform to make it possible for information from devices such as RFID-based locations, barcode-scan event, or device-reported data to be used with IBM's Blockchain and sync with distributed ledgers and smart contracts. It is a brave new blockchain-based world.

We claim:

1. A system for training an artificial intelligence system including the use of one or more human subject responses to stimuli as input to the artificial intelligence system comprising:

one or more displays, the display oriented to the human subjects to present the stimuli to the human subjects,

one or more detectors to monitor the reaction of the human subjects to the stimuli, the detectors including at least motion detectors, the detectors providing an output,

an analysis system, the analysis system coupled to receive the output of the detectors, the analysis system provides an output corresponding to whether the reaction of the human subjects was positive or negative, and

a neural network, wherein the output of the analysis system provides a:

positive weighting for training of the neural network when the output of the analysis system was positive, and

negative weighting for training of the neural network when the output of the analysis system was negative.

2. The system for training an artificial intelligence system of claim **1** wherein the neural network training is reinforcement learning.

3. The system for training an artificial intelligence system of claim **1** wherein the display is monitor.

4. The system for training an artificial intelligence system of claim **1** wherein the display is a virtual reality display.

5. The system for training an artificial intelligence system of claim **1** wherein the analysis system monitors individual behavior.

6. The system for training an artificial intelligence system of claim **1** wherein the analysis system monitors group behavior.

7. The system for training an artificial intelligence system of claim **1** wherein the detector is a motion tracking system.

8. The system for training an artificial intelligence system of claim **1** wherein the detector includes a facial detection system.

9. The system for training an artificial intelligence system of claim **8** wherein the facial detection system determines positive and negative facial attributes.

10. The system for training an artificial intelligence system of claim **1** wherein the detector further includes a sound detector.

11. The system for training an artificial intelligence system of claim **10** wherein the sound detector is a microphone.

12. The system for training an artificial intelligence system of claim **1** wherein the detector is a biometric scanner.

13. The system for training an artificial intelligence system of claim **1** wherein the detector is a physiologic detector.

14. The system for training an artificial intelligence system of claim **13** wherein the physiologic detector is a heart rate detector.

* * * * *

US 20180341861A1

(19) **United States**

(12) **Patent Application Publication**

KATZ et al.

(10) **Pub. No.: US 2018/0341861 A1**

(43) **Pub. Date: Nov. 29, 2018**

(54) **ARCHITECTURES, SYSTEMS AND METHODS FOR PROGRAM DEFINED STATE SYSTEM**

(71) Applicant: **MILESTONE ENTERTAINMENT LLC**, Beverly Hills, CA (US)

(72) Inventors: **RANDALL M. KATZ**, Beverly Hills, CA (US); **Robert Tercek**, Hollywood, CA (US)

(21) Appl. No.: **16/052,207**

(22) Filed: **Aug. 1, 2018**

Related U.S. Application Data

(63) Continuation of application No. 15/886,432, filed on Feb. 1, 2018.

(60) Provisional application No. 62/454,423, filed on Feb. 3, 2017.

Publication Classification

(51) **Int. Cl.**

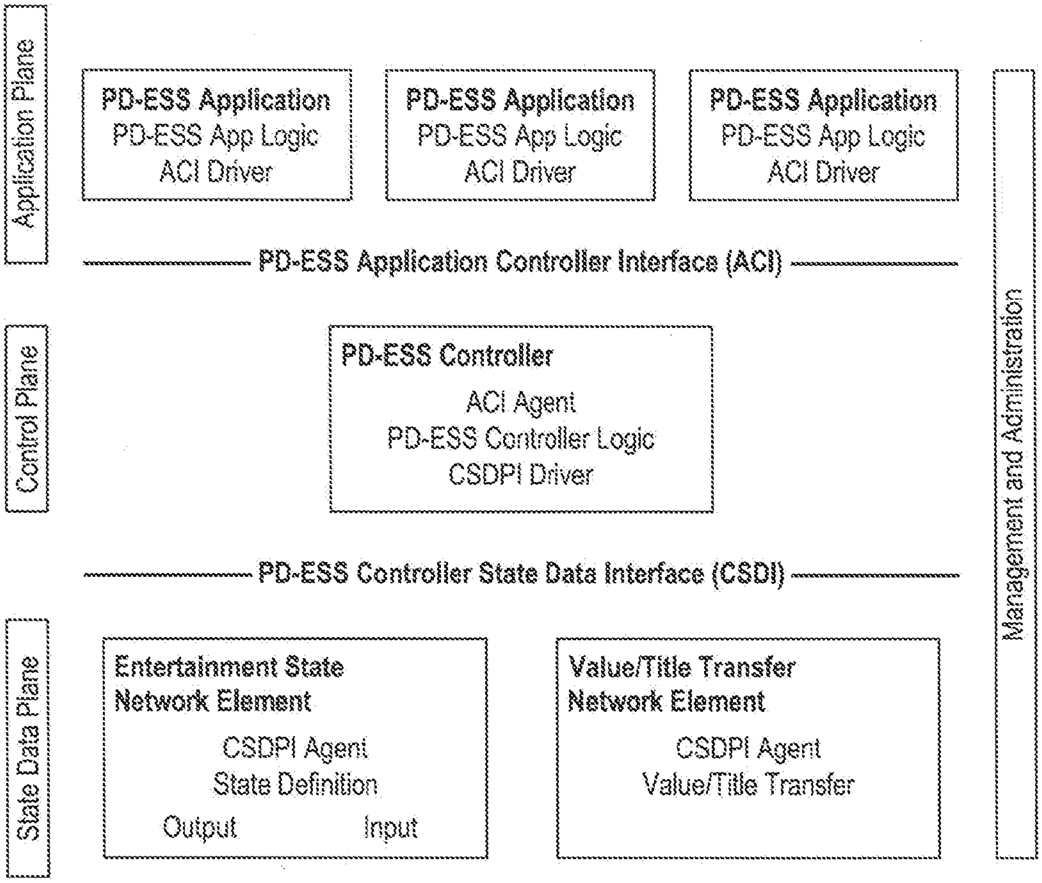
G06N 3/08	(2006.01)
G06K 9/00	(2006.01)
G07F 17/32	(2006.01)
G06Q 20/06	(2006.01)

(52) **U.S. Cl.**

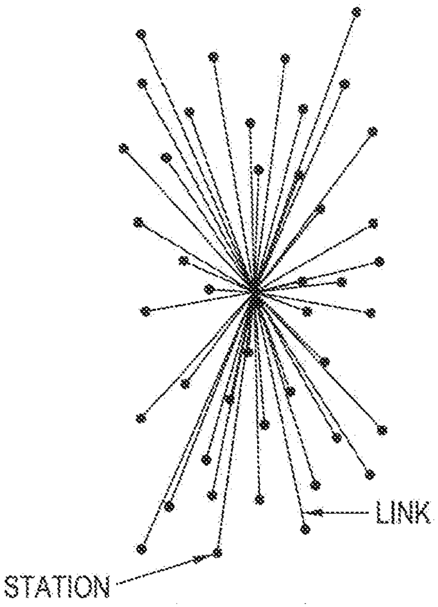
CPC ***G06N 3/08*** (2013.01); ***G06K 9/00221*** (2013.01); ***G06Q 20/065*** (2013.01); ***G07F 17/329*** (2013.01)

(57) **ABSTRACT**

In one aspect, the inventions include a system for control of an entertainment state system. First, an application plane layer is adapted to receive instructions regarding operation of the entertainment state system. Preferably, the application plane layer is coupled to an application plane layer interface. Second, a control plane layer includes an adaptive control unit, such as a cognitive computing unit, an artificial intelligence unit or a machine-learning unit. Third, a data plane layer includes an input interface to receive data input from one or more data sources.



Programmatically Defined Gaming System

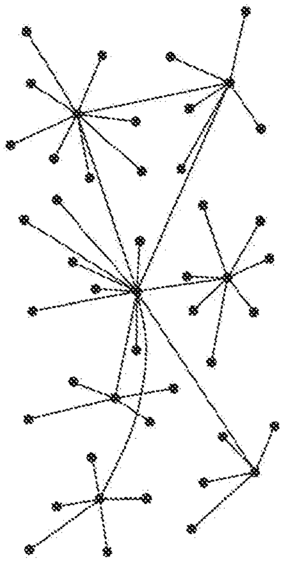


CENTRALIZED (A)

Prior Art Centralized System

FIG. 1

(Prior Art)

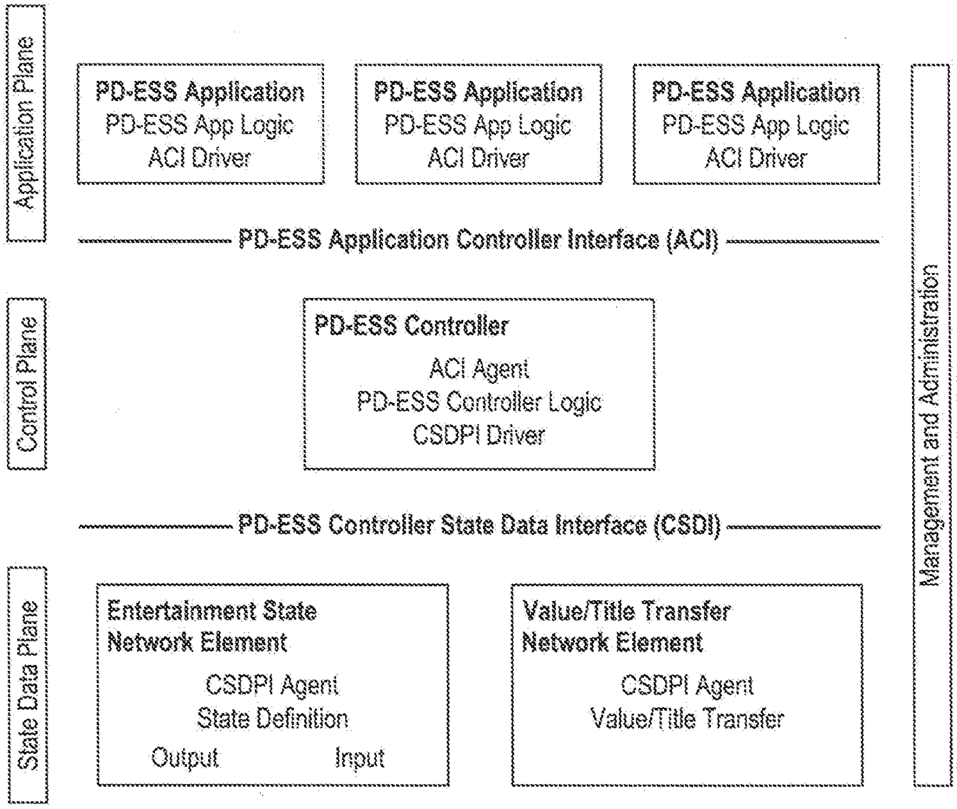


DECENTRALIZED

Prior Art Decentralized System

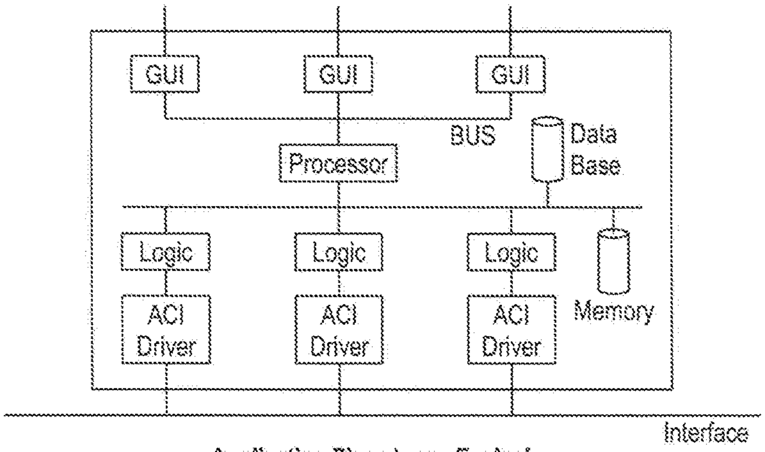
FIG. 2

(Prior Art)



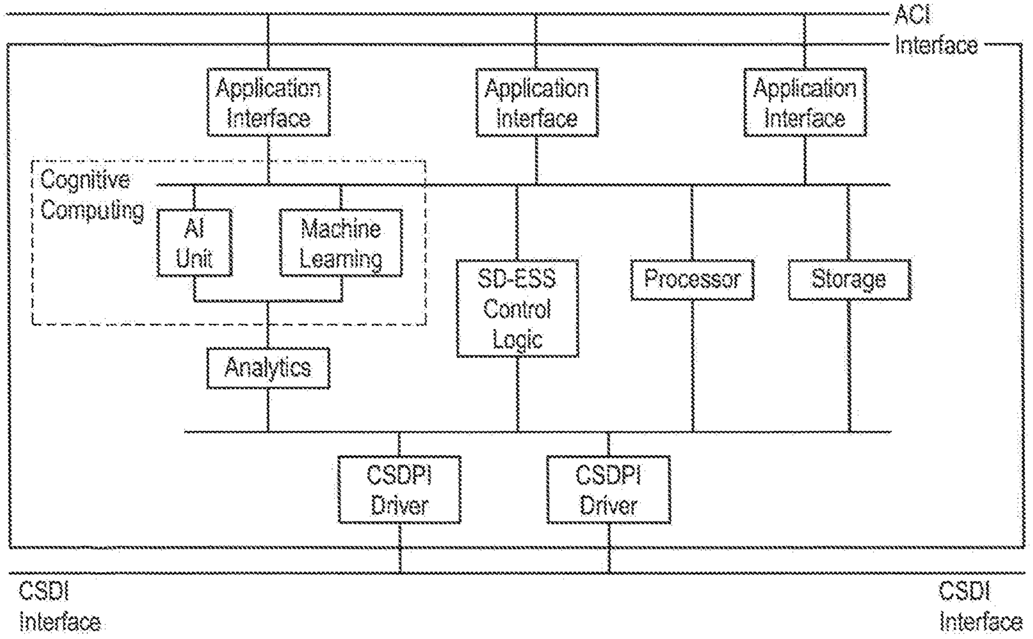
Programmatically Defined Gaming System

FIG. 3



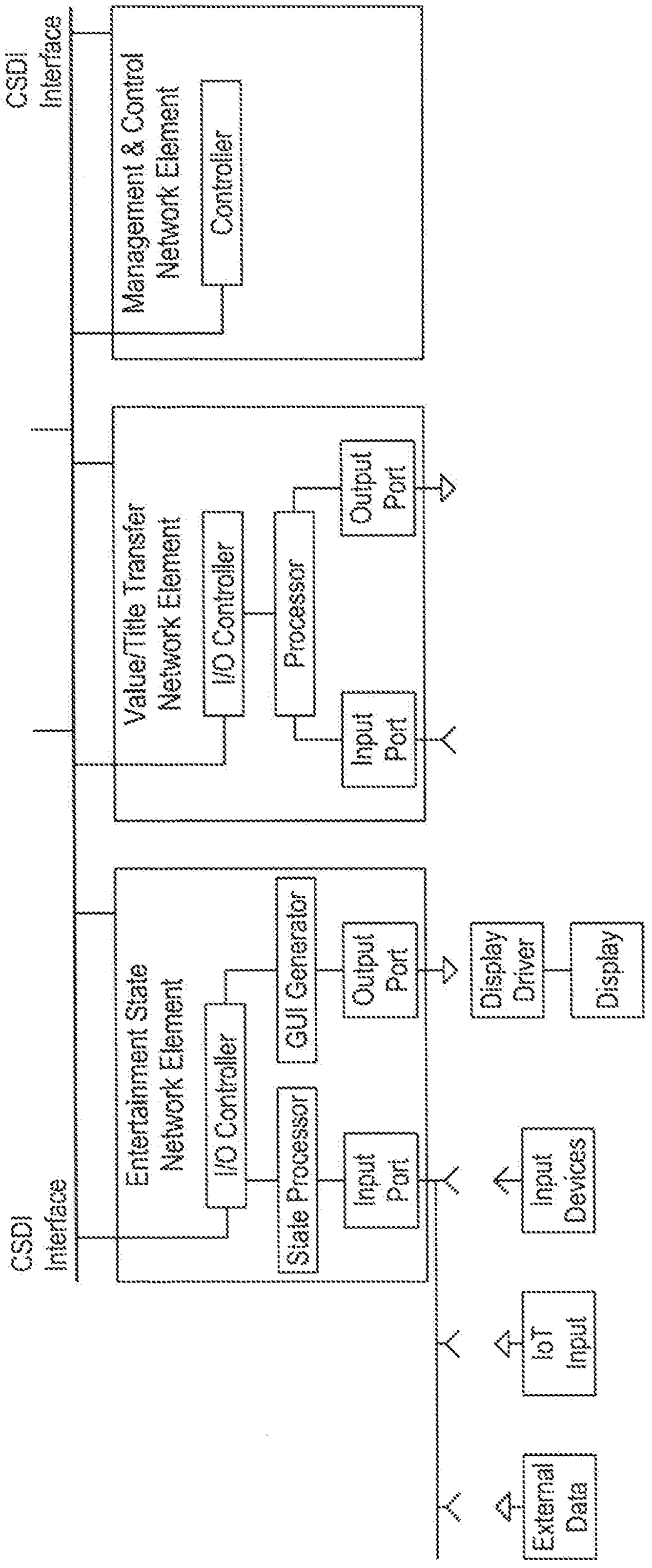
Application Plane Layer Explosion

FIG. 4



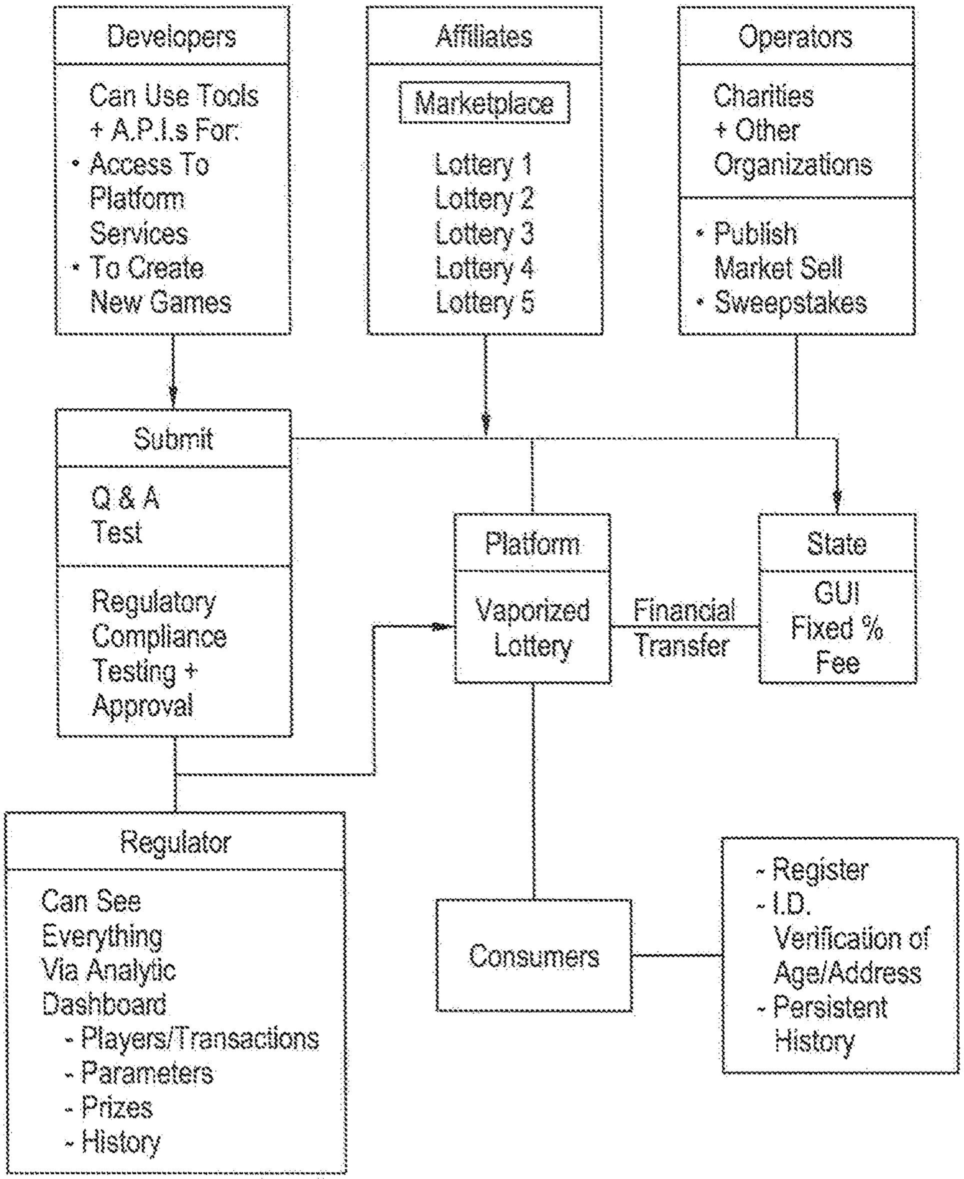
Control Plane Layer Explosion

FIG. 5



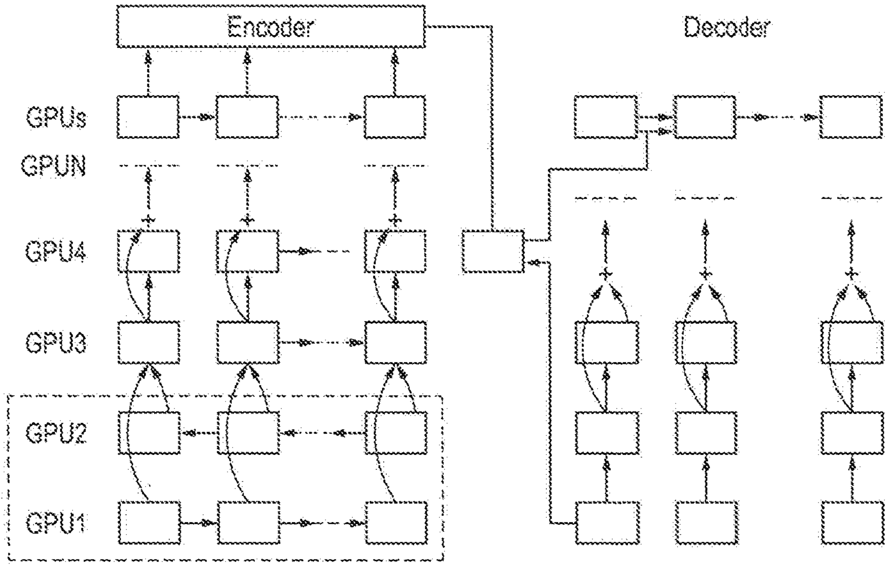
State Data Plane Layer Explosion

FIG. 6



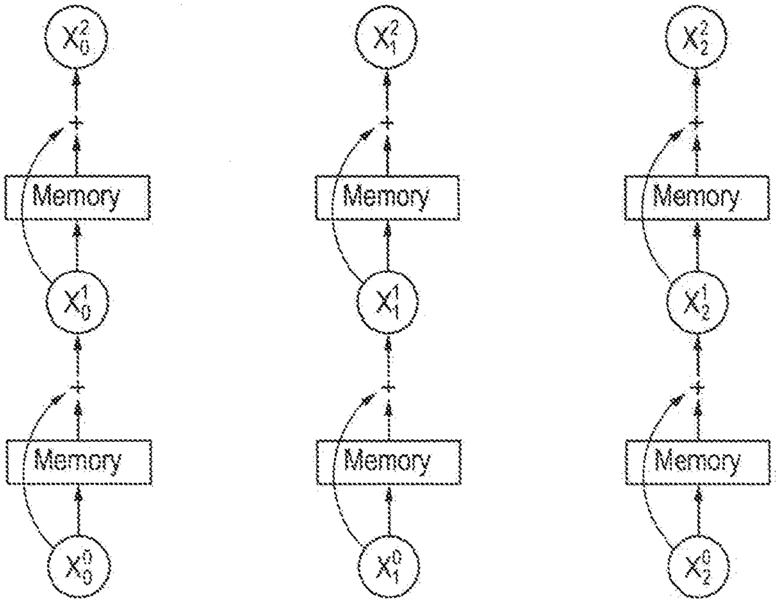
Ecosystem Interfaces and Interconnections

FIG. 7



Neural Network Model Architecture

FIG. 8



Neural Network

FIG. 9

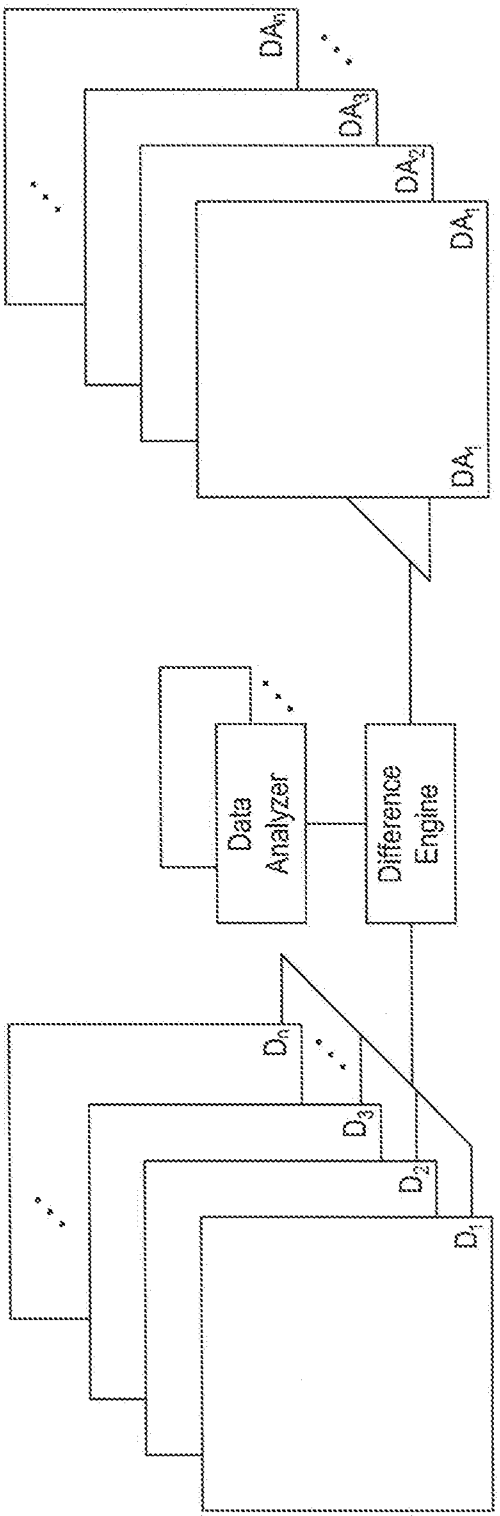

DAn
DA3
DA2
DA1
DA1
Data Analyzer
Difference Engine
Dn
D3
D2
D1

FIG. 10

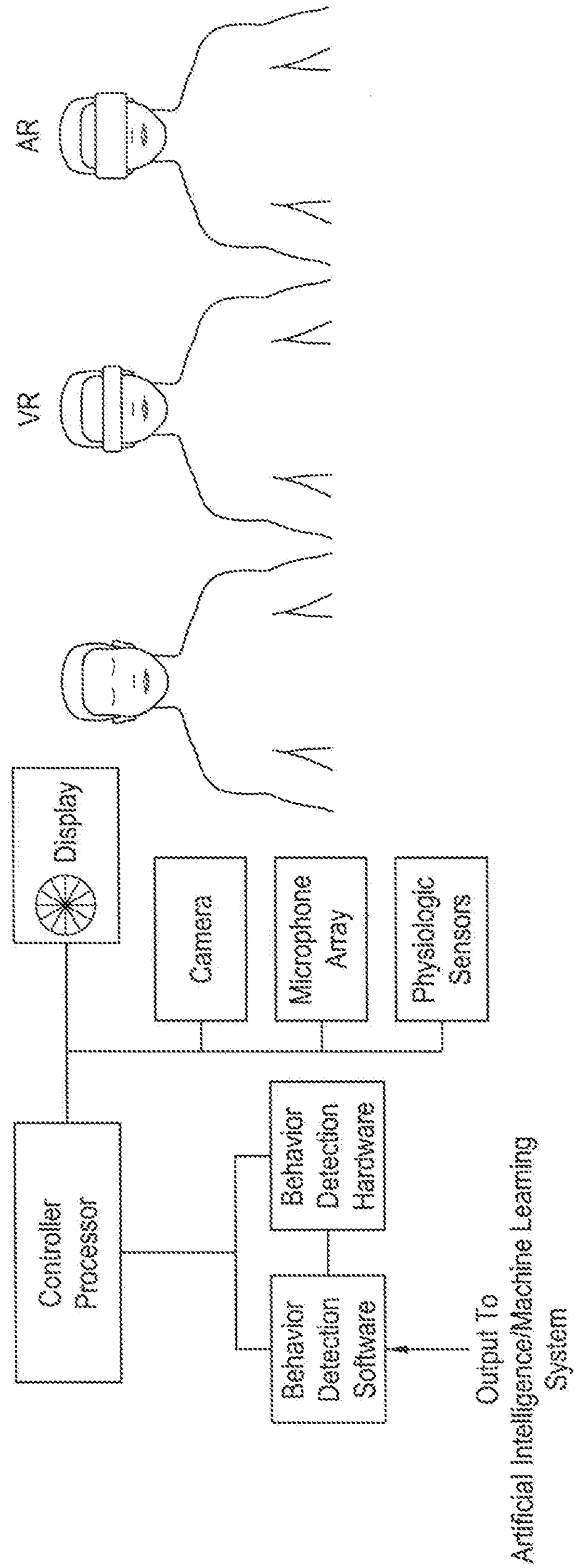
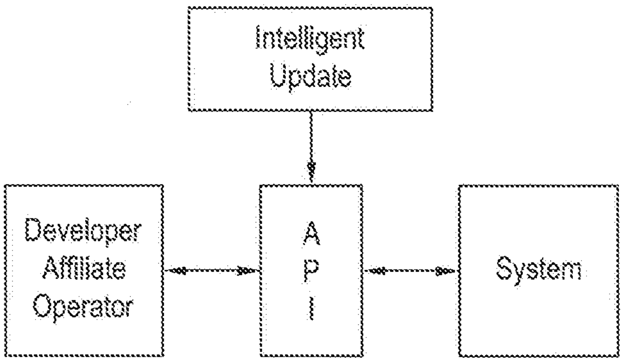
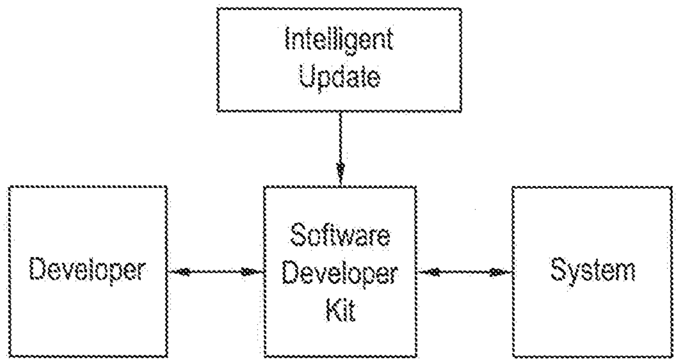

AR
VR
Display
Camera
Microphone Array
Physiologic Sensors
Controller Processor
Behavior Detection Hardware
Behavior Detection Software
Output To Artificial Intelligence/Machine Learning System

FIG. 11



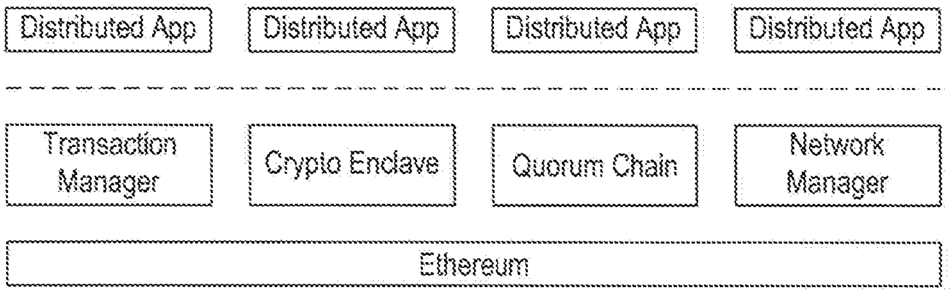
Dynamic Systems d-API

FIG. 12



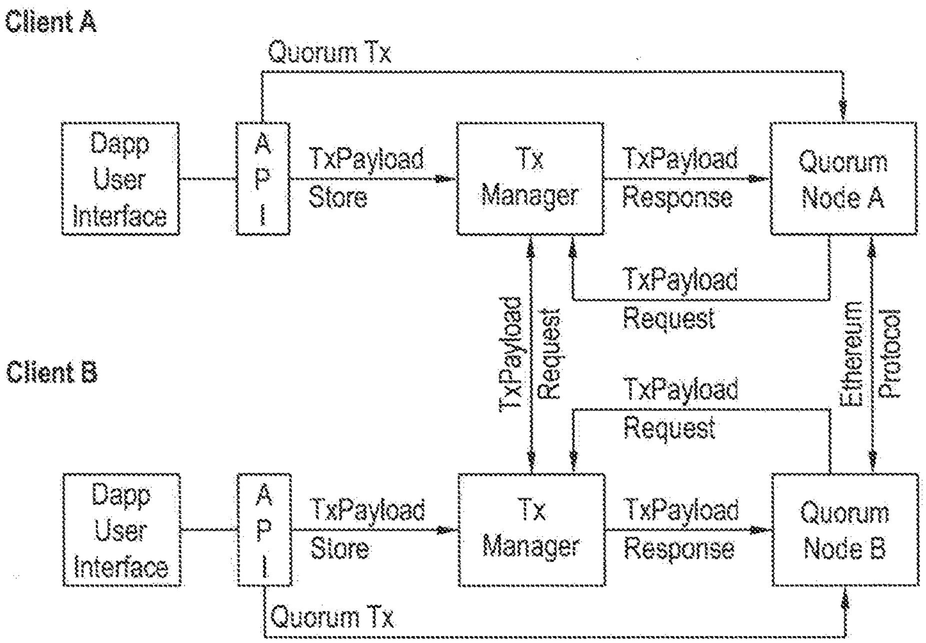
Dynamic Systems d-SDK

FIG. 13



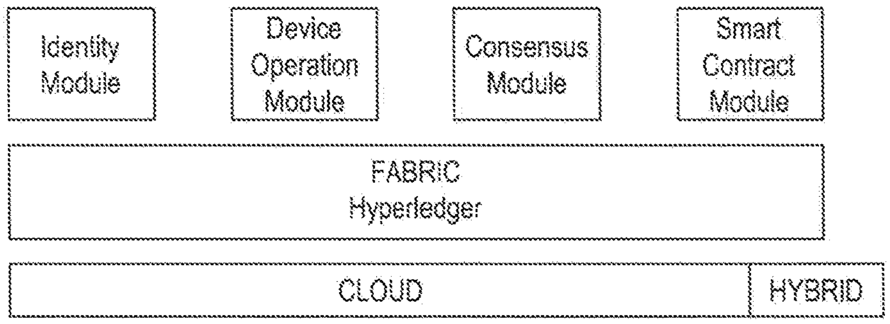
Architecture

FIG. 14



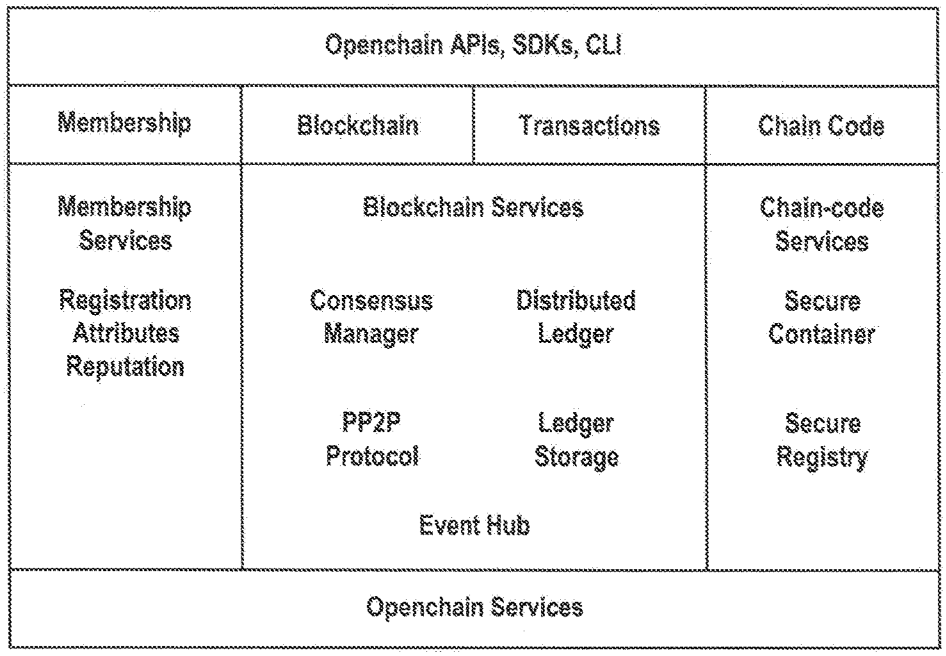
Permissioned System

FIG. 15



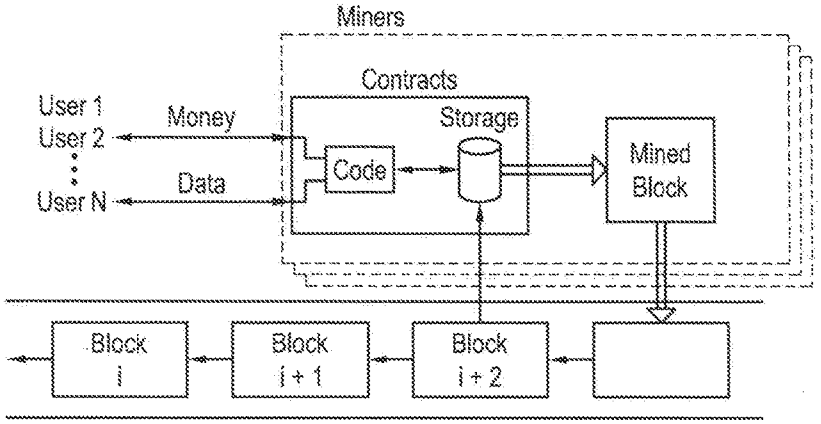
Blockchain Platform

FIG. 16



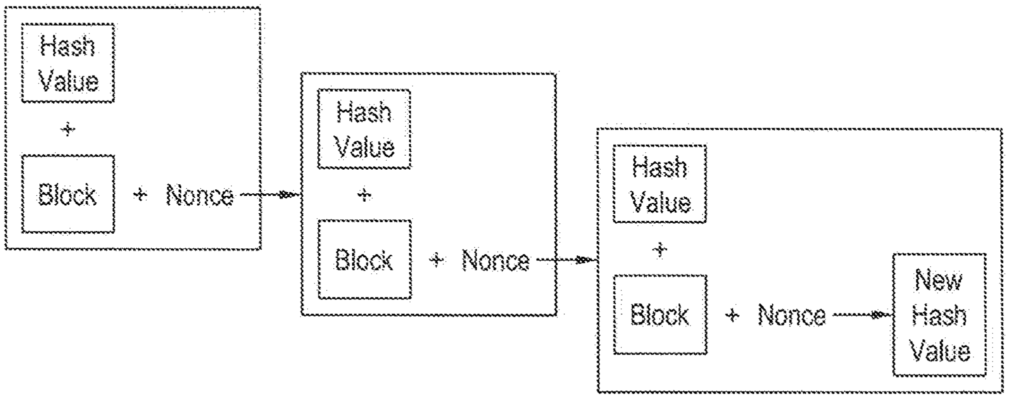
Platform

FIG. 17



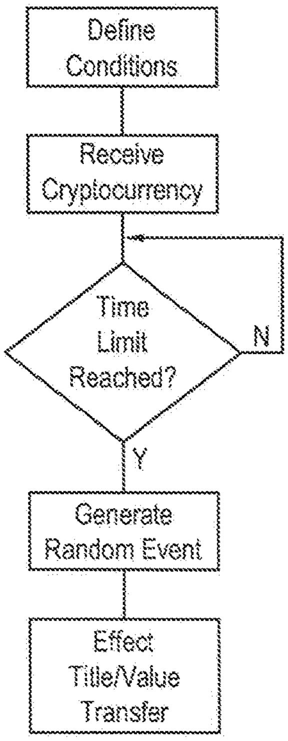
Schematic of a Decentralized Cryptocurrency System
with Smart Contracts

FIG. 18



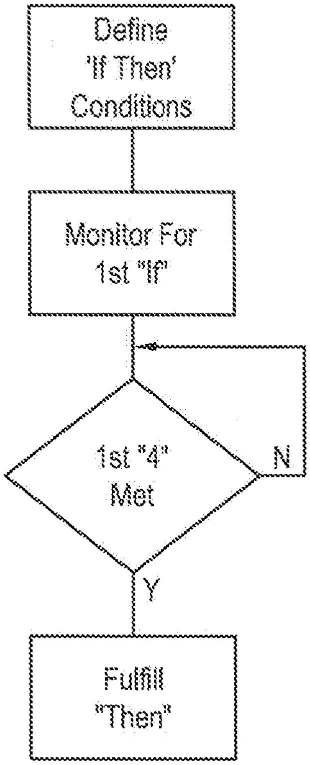
Schematic of Sequential Hash Value Creation
(Hash Value Plus Block Plus Nonce -> New Hash Value)

FIG. 19



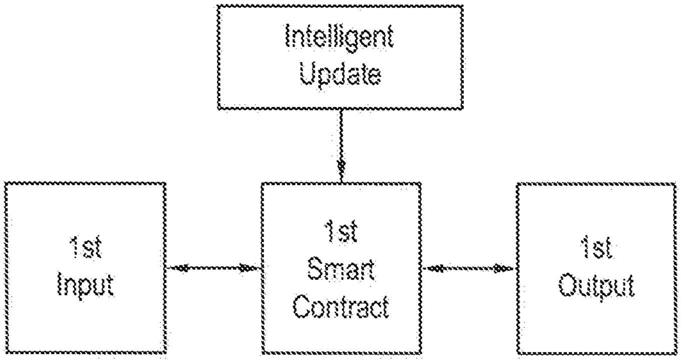
Flowchart for Crypto Currency Lottery

FIG. 20



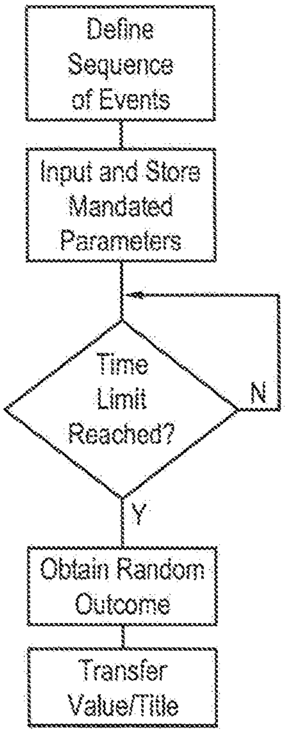
Smart Contract

FIG. 21



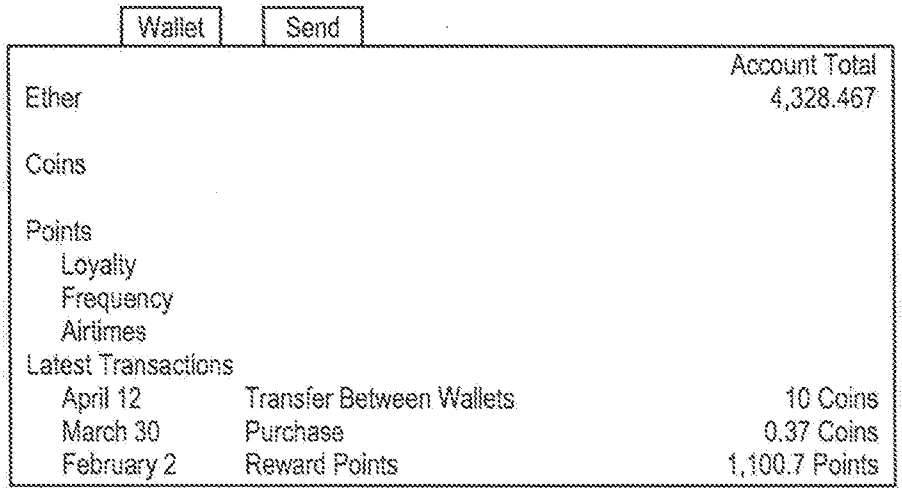
Smart-Smart (Smart^2) Contracts

FIG. 22



Smart Contracts with Mandated and Variable Parameters

FIG. 23



Account Total

Ether 4,328.467

Coins

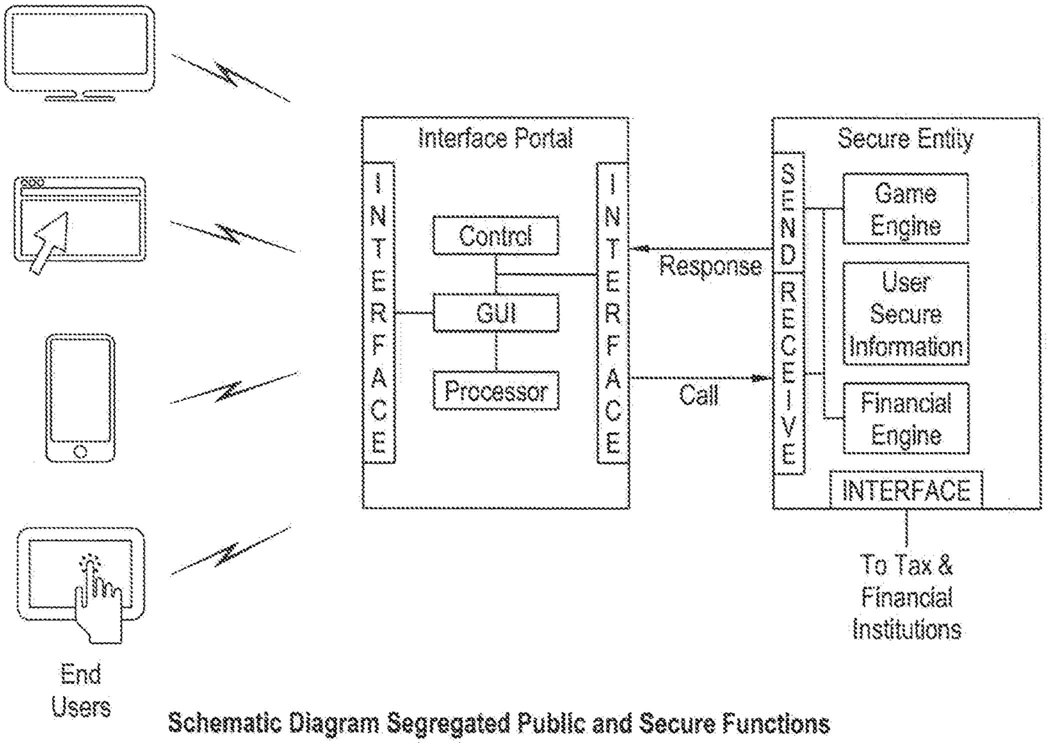
Points
- Loyalty
- Frequency
- Airtimes

Latest Transactions

April 12	Transfer Between Wallets	10 Coins
March 30	Purchase	0.37 Coins
February 2	Reward Points	1,100.7 Points

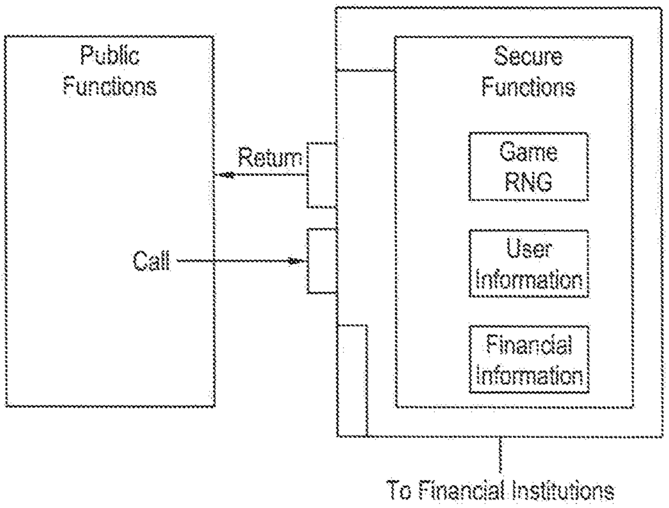
Cryptocurrency Wallet

FIG. 24



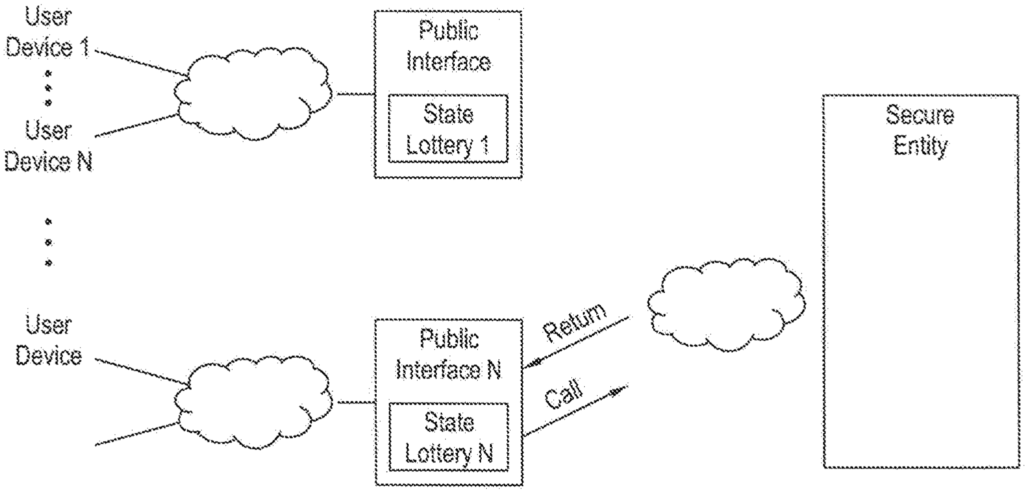
Schematic Diagram Segregated Public and Secure Functions

FIG. 25



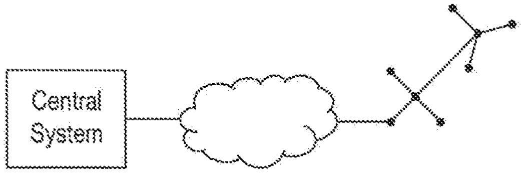
Interface of Segregated Secure and Public Functions

FIG. 26



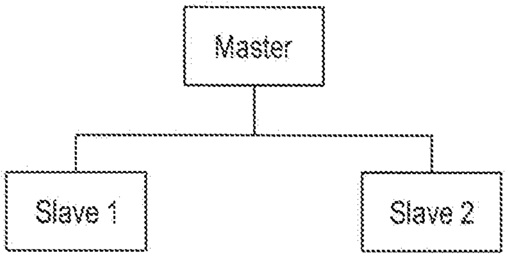
Network Implementation of Segregated Secure and Public Functions

FIG. 27



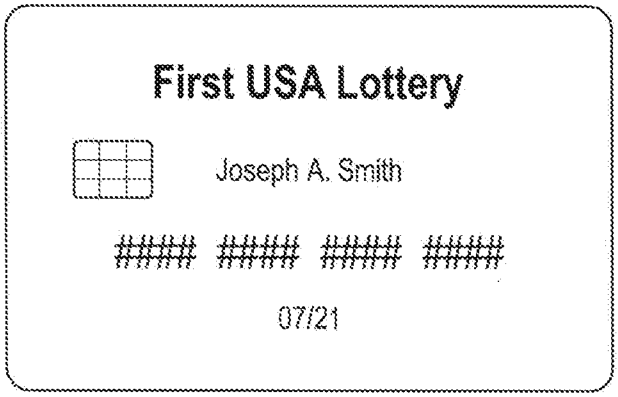
Centralized + Decentralized Systems

FIG. 28



Hierarchical Systems

FIG. 29



Lottery Linked Credit Card

FIG. 30

ARCHITECTURES, SYSTEMS AND METHODS FOR PROGRAM DEFINED STATE SYSTEM

PRIORITY CLAIM

[0001] This is a continuation of application Ser. No. 15/886,432; filed Feb. 1, 2018, which claims benefit of provisional Application No. 62/454,423, filed Feb. 3, 2017, which are incorporated herein by reference as it fully set forth herein.

FIELD OF THE INVENTION

[0002] The present inventions relate to architectures, systems and methods for programmatically controlled entertainment state systems. More particularly, architectures, systems and methods for program control utilizing cognitive computing, including but not limited to artificial intelligence and machine learning, and optionally including analytics. Systems, methods and architectures are provided for game and entertainment operations are provided utilizing decentralized systems, including block chain, optionally in peer to peer systems. More particularly, systems and methods for implementing a lottery, game or entertainment utilizing cryptocurrency, such as bitcoin, in a decentralized system.

BACKGROUND OF THE INVENTION

[0003] History shows that many trusted systems have evolved in order to provide for efficient functioning of society and business. Generally, these have involved central control of systems in order to ensure compliance with rules. Within the gaining space, examples include lotteries and regulated gaming. By way of example, the Nevada Gaming Control Board monitors institutions within the state for compliance with laws and regulations, and ensures the fair and efficient functioning of the industry.

[0004] Consider the entertainment and gaming system background. A lottery is a 'State' Function and serves as a loran of 'trusted agent'. The classic definition of the elements of a lottery are prize, chance and consideration. When these elements are reordered into a more chronologically correct order, namely first, receipt and holding of the consideration (e.g., ticket purchases), chance (e.g., ensuring a fair and accurate random number generator) and prize (i.e., paying the prize to the true winner.) Therefore, the State acts as a 'trusted agent' as it holds the consideration, guarantees randomness of the 'chance', and pays out the prize (title transfer). 'Trust' is based on the integrity and Trustworthiness of People Operating the System and the Regulators Who Oversee the System. Lotteries or State Regulators are often former law enforcement. The degree of trust in the. Regulators is often based on time and track record, the State of Nevada Regulatory system is considered highly trustworthy and effective, based in part on a multi-decade long track record. Additionally, a State with the most business to lose from a loss of trust in the regulatory process is most motivated to provide regulation. Such systems are based on central control of the system.

[0005] A casino is a 'state regulated' function and a form of 'trusted agent' with 'verification'. They are licensed by the State and subject to state inspection.

[0006] Various advancements have been made in the gaming and entertainment environment. The following are assigned to the assignee of this, and are hereby incorporated by Reference as if fully set forth herein: Games, And Methods For Improved Game Play In Games Of Chance And Games Of Skill, U.S. Pat. No. 6,565,084, Games, and Methods and Apparatus for Game. Play in Games of Chance, U.S. Pat. No. 6,488,280, Games, and Methods and Apparatus for Game Play in Games of Chance, U.S. Pat. No. 6,811,484, Apparatus and Method for Game Play in an Electronic Environment, U.S. Pat. No. 8,393,946, Apparatus, Systems and Methods for Implementing Enhanced Gaming and Prizing Parameters in an Electronic Environment, U.S. Pat. No. 7,798,896, Apparatus, Systems and Methods for Implementing Enhanced Gaming, and Prizing Parameters in an Electronic Environment, U.S. Pat. No. 8,241,110, Methods and Apparatus for Enhanced Play in Lottery and Gaming Environments, U.S. Pat. No. 8,727,853, Methods and Apparatus for Enhanced Interactive Game Play in Lottery and Gaming Environments, U.S. Pat. No. 8,241,100, Method and System for Electronic Interaction In A Multi-Player Gaming System, U.S. Pat. No. 8,535,134. Generally, they comprise a suite of tools to make systems more engaging, and to optimize results.

[0007] One vexing problem in larger systems results from systems incompatibility. Various components often come from various vendors. There is often a lack of interoperability and incompatibility. Various systems in the gaming ecosystem need to interoperate, including but not limited to: gaming operations, marketing, CRM (Customer Relationship Management), loyalty programs. Ancillary Points or Credits, System Analytics and Optimization, and account and audit functions.

[0008] Software Defined Systems are a collection of modules interoperated under a higher level of software control. These manage network services through abstraction of lower level functionality. Generally, there is an Application Plane, a Control Plane and a Data Plane. Examples include Software Defined Networks having a Control Plane which provides intelligent control of data plane composed of relatively less intelligent switches, routers, storage. Yet another example is software defined radio. The control plane monitors and supervises use of frequency bands in the data plane.

[0009] Yet another component is the use of static interfaces and tools. For example, APIs or Application Programming Interfaces generally comprise a static interface. They define a format for an information request. 'If you ask for X in a specific way, we will provide Y'. Genera no access is provided by requestor to the system other than via API. Yet another system are SDKs or Software Development Kit. They may be static. Tools are provided to achieve desired results. GDKs or Game Development Kit also may be static and provide tools for game development.

[0010] The design of entertainment or games is often driven by metrics driven design. This often involves A/B Testing comparing the results or favorability as between multiple systems. Further, they often monitor multivariate response systems.

[0011] One aspect of lotteries and Lotto style games is that they tend to be static. At the most extreme example, they are literally printed on cardstock. More generally, once a format for a lottery game has been chosen, such as a 6 out of 49 format, it is difficult to change. Public perception of change is that the game has become less favorable to the player.

[0012] Problem gambling issues have plagued the gaming industry. It is a significant issue for society. While users can solicit help (e.g., 1-800-Gambling), there is often denial and an unwillingness to seek help. Various attempts have been made to limit abuse, such as use rate limits in some on-line games.

[0013] In the move from bricks and mortar to on-line and cyber spheres, identity issues proliferate. Issues include: are you who you purport to be and will the user's identity be compromised?

[0014] Significant advances have been made in cognitive intelligence and adaptive intelligence. For example, IBM Watson won a Jeopardy competition 2011 against highly skilled players. Deep learning and pattern recognition has occurred. Current trends include big data, pattern recognition and machine learning.

[0015] Recent advances have also been made in object detection, both in 2D and 3D space. A challenge in the Large Scale Visual Recognition Challenge (LSVRC) provides for Object Detection in ImageNet 2016. The error rate of automatic labeling of ImageNet declined to less than 3%, compared to human performance of about 5%.

[0016] Significant advances have also been made in machine based game play performance. In 2015, Google DeepMind used an artificial intelligence reinforcement learning system to learn how to play 49 Atari games. In 2016, AlphaGo system from Google DeepMind beat one of the world's greatest Go players 4-1. In 2017, Carnegie Mellon University's Libratus program defeated top human players in a statistically significant manner.

[0017] Further advances have been made in cloud based systems. Functions have been migrating from local servers and storage to remote 'cloud' storage. These systems provide for easy scalability. Clouds based systems may run multiple 'instances' simultaneously. They also may combine software as a service, including Artificial Intelligence ("AI").

[0018] The Internet of Things ("IoT")) utilizes devices capable of sending data to remote location, and receiving command data. Various voice controlled devices use AI Or machine learning ("ML"), e.g. Amazon Alexa, Google Dot.

[0019] FIG. **1** shows an exemplary prior art centralized system. FIG. **2** shows an exemplary prior art distributed system.

[0020] Advancements have been made in trusted distributed systems such as in the use of blockchain based systems. The initial disclosure of the blockchain technology is attributed to Satoshi Nakamoto in a prier published October 2008. This system provides for automatic trust or system trust. The blockchain paradigm provides for a decentralized system utilizing decentralized consensus. This can be done in a peer-to-peer manner without an intermediary. The system may be viewed as a network of nodes running software on a programmable distributed network. It is sometimes referred to as a transaction singleton machine with shared state, a transaction based state machine, a message passing framework, a trustful object messaging compute framework and trusted computing.

[0021] A decentralized consensus is established by a combination of blockchain and cryptography. Authority and trust is provided by the decentralized virtual network. Consensus logic is generally separate from the application. It may comprise the first layer of a decentralized architecture.

[0022] Blockchain utilizes a distributed ledger. A 'block' comprises a new group of accepted transactions. A batch of transactions is released in a block to be validated by the network of participating computers. Continuous, sequential transaction record on a public block creates a unique "chain" or blockchain. This block is published to all other nodes. The publication occurs periodically, e.g. every 10 minutes.

[0023] Etherium is an open source platform for smart contracts. As currently operated, Etherium is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference.. The applications run on a custom built blockchain, an extremely powerful shared global infrastructure that can move the value and represent ownership of the property. This allows developers to create markets, store debt or promise records, move funds according to long-standing instructions (such as a will or a futures contract), without the counterparty risk. Etherium also states that its goal is to create a tradeable digital token that can be used as a currency, a representation of an asset, a virtual share, a proof of membership or anything at all. These tokens use a standard coin API, so the contract will be automatically compatible with any wallet, other contract or exchange also using this standard. The total amount of tokens in circulation can be set to a simple fixed amount or fluctuate based on any programmed ruleset. In summary, Etherium states that it enables building a tradeable token with a fixed supply, a central bank that can issue money and a puzzle-based cryptocurrency.

[0024] There are many disadvantages to the current systems. They are slow to change and innovate. They often involve proprietary systems that do not interoperate. There is often governmental and or institutional bias. There may be a cumbersome regulatory environment. Finally, there are often high transaction costs.

[0025] Thus, there is a need for interoperability among inconsistent, often proprietary systems. There is a need for gambling limitation on a more global basis, including geo-limitation and global use rate monitoring for problem gambling. There is a need for problem gambling detection and remediation. There is a need for improved distributed systems

SUMMARY OF THE INVENTION

[0026] In one aspect, the inventions include a system for control of an entertainment state system. First, an application plane layer is adapted to receive instructions regarding operation of the entertainment state system. Preferably, the application plane layer is coupled to an application plane layer interface. Second, a control plane layer includes an adaptive control unit, such as a cognitive computing unit, an artificial intelligence unit or a machine-learning unit. Third, a data plane layer includes an input interface to receive data input from one or more data sources.

[0027] Systems and methods are provided for training an artificial intelligence system including the use of one or more human subject responses to stimuli as input to the artificial intelligence system. One or more displays are oriented toward the human subjects to present the stimuli to the human subjects. One or more detectors serve to monitor the reaction of the human subjects to the stimuli, the detectors including at least motion detectors, the detectors providing an output. An analysis system is coupled to receive the output of the detectors, the analysis system providing an output corresponding to whether the reaction of the human subjects was positive or negative. A neural network utilizes the output of the analysis system to provide a positive weighting for training of the neural network when the output of the analysis system was positive, and a negative weighting for training of the neural network when the output of the analysis system was negative.

BRIEF DESCRIPTION OF THE DRAWINGS

[0028] FIG. **1** is a diagrammatic view of a prior art centralized system.

[0029] FIG. **2** is a diagrammatic view of a prior art centralized system.

[0030] FIG. **3** is a system level block diagram of the program defined entertainment state system (FD-ESS) showing the application plane, the control plane and the state data plane.

[0031] FIG. **4** is a system level block diagram explosion of the application state plane layer of the PD-ESS.

[0032] FIG. **5** is a system level block diagram explosion of the control plane layer of the PD-ESS.

[0033] FIG. **6** is a system level block diagram explosion of the state data plane layer of the PD-ESS.

[0034] FIG. **7** is a diagrammatic view of the ecosystem, including interfaces and interconnections.

[0035] FIG. **8** is a system level block diagram of the neural network model architecture including graphical processing units (GPUs).

[0036] FIG. **9** is a system level block diagram of the neural network model architecture.

[0037] FIG. **10** is a system level diagram of multiple data sets including a difference engine and data analyzer.

[0038] FIG. **11** is response system display and detection system for generating input to train the artificial intelligence (Al) and machine learning (ML) systems.

[0039] FIG. **12** is a system level diagram of a dynamic system application programing interface (d-API).

[0040] FIG. **13** is a system level diagram of a dynamic software development kit (d-SDK).

[0041] FIG. **14** is a system architecture level diagram of a distributed system including blockchain and Etherium,

[0042] FIG. **15** is a system architecture level diagram of a permissioned blockchain system,

[0043] FIG. **16** is a system architecture level diagram of a blockchain platform.

[0044] FIG. **17** is a system architecture level diagram of a blockchain platform including open chain services.

[0045] FIG. **18** is a system architecture level diagram of a decentralized cryptocurrency system with smart contracts.

[0046] FIG. **19** is a system architecture level diagram of a decentralized system with sequential hash value creation.

[0047] FIG. **20** is a flowchart diagram of a cryptocurrency lottery.

[0048] FIG. **21** is a flowchart diagram of a smart contract.

[0049] FIG. **22** is a flowchart diagram of a smart-smart (smart^2) contract.

[0050] FIG. **23** is a flowchart diagram of a smart contract having mandated and variable parameters.

[0051] FIG. **24** is a graphical user interface (GUI) of a cryptocurrency wallet.

[0052] FIG. **25** is a system architecture level schematic diagram of a system having segregated public and secure functions.

[0053] FIG. **26** is a system architecture level of an interface of segregated public and secure functions.

[0054] FIG. **27** is a system architecture level of a network implementation of a system having segregated public and secure functions.

[0055] FIG. **28** is a system architecture level of a combined centralized and decentralized system.

[0056] FIG. **29** is a system architecture level of a hierarchical system.

[0057] FIG. **30** is a plan view of a lottery linked credit card.

DETAILED DESCRIPTION OF THE INVENTION

[0058] Architectures, Systems and Methods for Program Defined Entertain men State Systems

[0059] The following description is primarily in connection with FIGS. **3**, **4**, **5** and **6**, but may apply to other figures as well. AR architecture is provided for a program defined entertainment state system. This preferably serves to decouple the system that controls the overall experience from the underlying systems that define states. The first plane, the application plane provides an interface, primarily for system side users, e.g., developers, organizers of events contests, lotteries. The second plane, the control plane, provides for intelligent control, especially cognitive computing, including artificial intelligence and/or machine learning, including artificial intelligence where the system learns over time. Tins preferably provides an intelligent control layer above modules. The third plane, the state data plane, provides for entertainment 'state modules' with various mechanics, preferably including 'core loop', meta states and provides interfaces for end users, as well as inputs and outputs.

[0060] FIG. **3** provides a block Diagram Program Defined Entertainment State System (PD-ESS). FIG. **4** is an Explosion of PD-ESS Application Plano Layer, including an application layer GUI (facing the Developers, Affiliates, and Charities). FIG. **5** provides an. Explosion Pi) ESS controller plane layer. FIG. **6** provides an explosion PD-ESS state data plane layer. Also included are an explosion of entertainment state network element layer, a user interface GUI, an explosion of value/title transfer network element and explosion of other functional blocks.

[0061] Turning first to the Application Plane Layer, a program serves to communicate requirements and desired behavior to the PD-ESS Controller, it provides communication between the PD-ESS Application and PD-ESS Controller via the PD-ESS Application Controller Interface (ACI). Application Logic and Drivers are optionally provided. The application layer may receive an abstracted view of State Data Plane Actions. The PD-ESS Applications may interface with higher levels of abstracted control. The system includes an interface, the PD-ESS Application Controller Interface (ACI). The management and administration preferably provides the following: (1) To/From Application Plane, it provides contracts and SEAS, (2) To/from Control Plane Configure Policy, Monitor Performance, and (3) To/From Data Plane Element Setup.

[0062] Turning second to the Control Plane Layer, the PD-ESS Controller is ideally logically centralized entity, preferably serves to translate the requirements of the PD-ESS Application to the State Data Plane layer, and provides the Application layer with actions in the State Data Plane (e.g. event information and statistical information). The control plane may provide statistics, events and states from the Data Plane to the Application Plane. The control plane preferably enforces behavior at a low level control in the data plane, provides capability discovery, and monitors statistics and faults. The control plane advantageously includes cognitive computing, such as artificial intelligence (AI) and machine learning (ML), to be described in greater detail, below.

[0063] The control plane may optionally include analytics, including but not limited to pattern recognition. Analytics may be performed on a population preferably a relevant population, or on a subset. Preferably, the subset has similar characteristics of a target user. Data may be binned according to subset. The scope of primary data may be analyzed. Predictive modeling may be included. Responsible Gaming Control may be implemented at the control plane level, especially if there are use rate limits and global limits.

[0064] Turning thirdly to the state data plane layer, it preferably includes main subcomponents and Functional Network Elements. Optionally, the functional network elements include some or all of the following: 1. Entertainment State Network Elements, 2. Value/Title Transfer Network Element, 3. Game Library, such as Casino, VLT, Video Gaming, Tournament, Amusement with Prize (AWP), Game Mechanics, Core Loop, Skill, Skill with Reveal, Second Chance, Social, Gamification, Prizing, vGLEPs and Prize Board, 4. Systems, Marketing, Promotions, CRM, Operations, Logistics, Interactive. Mobile/Apps and Responsive Design, 5. Platforms, 6. Channels, 7, Lottery, including Retail and Central Systems, 8. Loyalty, 9. Responsible Gaming Control, optionally including use rate limits and global limits (may be done in the control plane layer as well), 10, Sports, including real world, fantasy and eSports 11. Other Live Data Entertainment, 12. Networks, including Network communications and web services and 13, Management, including Records, Player Account Management, Reporting, Compliance, including regulatory compliance, security, including cybersecurity, fraud and risk management, including preferably audit and payment.

[0065] The Entertainment State Network Elements provide an interface for interaction with a user of the system. An input receives information from user selection. Sensors may be of various forms, including sound sensors, motion sensors, whether 2-d or 3-d, such as including the Microsoft Kinect system. 'Internal Data' consists of data related primarily to game operations. 'External' Data sources to combine with Primary Data Source. These may include 1. Location, 2. Current Activity such as Driving (provided by vehicle, provided by tracked phone) or Exercising (provided by FitBit or similar), 3. Economic. Conditions, 4. Weather, 5. Recent Events/News, e.g., a recent Large PowerBall win, 6. Marketing Information, 7. e-mail scans, e.g., Google scanning of Gmail for content, 8. Social Media, and 9. the Internet of Things (IoT). The Internet of Things (IoT) provide various forms of connected devices such as data sensors. The sensors generate data input "stimuli" to system. By utilizing any form of input, the system is able to provide for massive parallelism. All data "stimuli" to system permits the system to be adaptive and reactive to all data stimuli.

[0066] An Output provides stimulation to user. Forms may include: 1. images, such on a display, or via a GUI, or VR system, AR system, 2. Thin Client display with remote computing power, 3. Projections and Holograms, 4. sounds, 5, tactile stimuli, 6. olfactory stimuli, or 7. direct electrical stimuli, neural or otherwise.

[0067] A Value/Title Transfer Network Element serves to receive and transfer value (money, coins, and other items of value), Value may refer to fungible liquid asset or other store of value. Title generally refers to ownership of real, personal, or virtual property. A detailed discussion of blockchain, trust-less, and cryptocurrency systems is provided, below.

[0068] Artificial Intelligence (AI) is broadly that branch of computer science dealing in automating intelligent behavior. They are systems whose objective is to use machines to emulate and simulate human intelligence and corresponding behavior. This may take many, forms, including symbolic or symbol manipulation AL it may address analyzing abstract symbols and/or human readable symbols. It may form abstract connections between data or other information or stimuli. It may form logical conclusions. Artificial intelligence is the intelligence exhibited by machines, programs or software. It is has been defined as the study and design of intelligent agents, in which an intelligent agent is a system that perceives its environment and takes actions that maximize its chances of success. Yet others have defined it as the science and engineering of making intelligent machines.

[0069] Artificial Intelligence often involves use of neural networks. In various embodiments, a multi-layer stack of neural network nodes are utilized. The lowest level comprises granular elements. By way of example in a gaming application, in the order of higher level understanding, the levels would progress from instances of individual action (granular), to core loop detection, to session play, to multisession play. Optionally, a parsing engine serves to break down or subdivide a larger set, such as a data set or image, into more discrete or granular elements.

[0070] AI may have various attributes. It may have deduction, reasoning, and problem solving. It may include knowledge representation or learning. Systems may perform natural language processing (communication). Yet others perform perception, Motion detection and information manipulation. At higher levels of abstraction, it may result in social intelligence, creativity and general intelligence. Various approaches are employed including cybernetics and brain simulation, symbolic, sub-symbolic, and statistical, as well as integrating the approaches.

[0071] Various tools may be employed, either alone or in combinations. They include search and optimization, logic, probabilistic methods for uncertain reasoning, classifiers and statistical learning methods, neural networks, deep feedforward neural networks, deep recurrent neural networks, deep learning, control theory and languages.

[0072] AI advantageously utilizes parallel processing and even massively parallel processing in their architectures. Graphics Processing Units (G Us) provide for parallel processing. Current versions of GPUs are available from various sources, e.g., Nvidia, Nervana Systems.

[0073] Machine Learning is defined as a system that builds up knowledge from experience, Machine learning serves to detect patterns and laws.

[0074] Deep Learning uses Neural AI. It is easily scalable, and typically involves more layers or neural Networks (NNs), Neural Networks may be of various forms, including: efficient NN, vectorized NN, vectorized logistic regression, vectorized logistic regression gradient output, binary classification, logistic regression, logistic regression cost function, gradient descent, derivatives, computation graph and logistic regression gradient descent.

[0075] Deep neural networks (DNN) often involve hyperparameter tuning. Typically they utilize regularization and optimization. Sometimes they are referred to as Deep Belief Network (DBN).

[0076] Other forms of neural networks include Convolutional Neural Networks (CNN) or Recurrent Neural Networks (RNN), Examples of available systems include: LS™, Adam, Caffe, Dropout, Batch Norm, Xavier/He, Python, Scikit-Learn and TensorFlow.

[0077] AI may operate on various forms of data sets. The data set may comprise images, whether video images, 2D Data and/or 3D Data. Sequential data may be analyzed. Examples include, but are not limited to, natural language, audio, autonomous driving decisions, game states and game decisions.

[0078] Various industry applications advantageously benefit from application of AI. They include imaging and object detecting, serving to identify, classify, mining and optionally provide sentiment analysis. Other applications include autonomous driving. Yet other applications include robots and robotics. Within healthcare, functions include imaging analysis, diagnosing and gamification. Various forms of sequential data analysis may be enhanced, such as speech recognition, and natural language processing. Music applications include both recognition and synthesis. Within the gaming field, applications include game state sequences detection, analysis, formation, combination optimization, and game optimization. Chat hots and machine translation advantageously employ these systems.

[0079] FIG. **7** shows the constituent function blocks within an entertainment or gaming ecosystem. Affiliates serve to acquire customers. Affiliates receive a commission, such as based on the number of users acquired or a percent (%) of revenue. Optionally, there is a link to a credit card function (to be discussed, below in connection with FIG. **30**).

[0080] Next are charities and other organizations that plan to operate a lottery, game or other entertainment event. They provide for customer acquisitions. They are the recipient of the event (game, lottery or entertainment). They also collect a fee.

[0081] Next are the developers, who provide for game design. In return for game design, they receive multi-jurisdictional use and payment for use. An enhanced application or app store may be provided wherein the game design may be viewed, selected and downloaded.

[0082] Next, consumers provide registration and identification information. The registration data may optionally include identification, age, address and verification. Optionally, the data is sufficient that the system can comply with Know Your Customer (KYC) rules, with optional levels of identity verification. This is stored as persistent history. The customer receives a chance to play, win, and receive entertainment.

[0083] Next is the regulator or trust verifying agent. They provide testing, approval for game fairness, overall approval, ensure compliance with regulations and security. The regulator or trust verifying agent is granted access permission by the system to monitoring of every transaction, (analytics dashboard), player accounts, parameters, prize amounts and payouts, and to the complete history. The regulator or trust verifying agent receives compensation, whether a fee or as a percentage of the transaction amounts.

[0084] Next, the lotteries serve as the trusted agent, and receive a percentage of the transaction amount. Optionally, the historical functions of the lottery may be eliminated or vaporized from the system when those functions arc performed by another entity within the ecosystem.

[0085] FIGS. **8** and **9** relate to the learning processes for training neural networks. By providing repeated input stimulus and then training the neural network to provide the correct output, the system may be taught to form the correct associated output based On one or more input stimului. In converting input to the desired output the training may comprise supervised learning, such as when the target values and parameters are supervised. Alternatively, the training may be non-supervised learning, wherein the system attempts to identify patterns in the input that have identifiable structure and can be reproduced. Alternately, the system may use reinforcement learning, which works independently (like non-supervised learning) but is rewarded or punished depending on success or failure. Preferably, reinforcement learning involves incremental change. In the various training techniques, perturbation may be used wherein one or more input parameters are varied, typically in a perturbation amount, e.g., less than 10%, more preferably less than 5%, and most preferably less than 3%, of the input value, so as to monitor the effect of the perturbation on the output.

[0086] Hyper parameters and parameters may be used in the AI or machine learning systems. Model parameters are estimated from data automatically. A configuration variable internal to the model can be estimated from data. This can be required by the model when making predictions. Values define the skill of the model. They may be estimated or learned from data.

[0087] Hyperparameters are set manually and are used in the processes to help estimate parameters. A configuration variable external to the model is used. Generally, it, cannot be estimated from the data. They are often used in processes to estimate model parameters. They are typically specified by the system user. Hyperparameters can often be set using heuristics. They are often tuned for a given predictive modeling problem. A hyperledger may be used, either as a hyperledger composer or hyperledger fabric.

[0088] The AI or machine learning may be performed on, various types of hardware. Advantageously, systems that support parallel processing can provide for computation speed and efficiency. Parallel processing units such as Graphics Processing Units (GPUs) are available from NVIDIA and AMD. Neural Processing Units (NPUs) are available in the Kirin 970, Apple A11 and the Qualcomm Zeroth Processor. AI and machine learning processing is also available as a cloud AI or Machine learning system, such as is available from Google and Amazon Web Services.

[0089] FIG. **10** describes domain transformations and difference engines. One advantageous domain transformation involves the time domain to frequency domain (time series to frequency domain). One example is the Fourier series, which generally is used with repetitive signals, such as oscillating systems. A Fourier transform, is generally used with non-repetitive signals, such as transients. Enhanced computational techniques such as the Fast Fourier Transform (FFT) may be used for efficiency and computational speed. Yet, another domain transformation is the Laplace transform, often used in electronic circuits and control systems. Yet another, the Z transform, is used with generally discrete-time signals. Digital Signal Processors (DSPs) may be advantageously utilized. Spectral density estimation may be included, along with wavelet analysis, image analysis, data compression and multivariate analysis. Correlated data sets are advantageously employed.

[0090] Difference engine may be employed to identify differences between two or more sets of data. The difference may be time based, such as where one data set relates to a time **0**, and the other set relates to a time **1**, time **2**, time **3**, . . . , time N. Differences in images may be calculated.

[0091] FIG. **11** shows a system in which the Subject response may be monitored, captured and analyzed for behavior, which is then used as input to AI. In various efforts, such as in game or entertainment design and creation, the response of the target audience may be monitored, analyzed and used to train an Artificial Intelligence or machine learning system. The subject response to entertainment/game stimuli serves to measure the 'fun' experienced by the subject, and that measure (the 'fun') is then used as a training input to AI or ML system. The system may detect individual subject behavior. Alternatively, the system may monitor group behavior, serving to detect the 'fun' experiences, but may also measure attributes of the group or crowd, such as 'excitement', 'engagement' or crowd based behavior.

[0092] A display is provided as a stimulus to the subject or subjects. A that panel display or monitor may be utilized. Optionally, personal viewing devices may he utilized, such as individual screens, virtual reality headsets, augmented reality devices, heads up displays, projection devices or imaging technology.

[0093] Various detectors are utilized to monitor the one or more subject's response. Motion detection utilizes motion tracking hardware and software. A camera images the subjects. Various cameras include the Microsoft Kinect, 2d sensors and cameras and 3d sensors and cameras. Metrics detectors may analyze the position of a body part, such as a limb, joint or facial feature. It may measure the velocity, movement, higher level derivatives of the position or movement, such as the rate of change of change. Facial detectors monitor for facial recognition. Facial attributes may be detected, such as positive attributes, e.g. a smile, or negative attributes, e.g., a frown. Body position detection may be determined. Sound detection may be performed with a microphone or microphone array. It may detect attributes of the sound, such as positive attributes, e.g., a cheer, and negative attributes, e,g., expletives, and boos. Biometric scan detection is utilized. Physiologic response detection optionally monitors the subject heart rate, blood pressure, pupil dilation, temperature, ECG, and mental activity. Activity monitoring detectors monitor engagement response, preferably including bet rate, time spent engaged with the display, retention rate, repetition rate and reengagement rate. Analytics are advantageously utilized.

[0094] The output of the system is used as input in the AI or machine learning system. For example, in training using reinforcement learning in neural networks, a positive weighting is used for positive attributes, and a negative weighting is used for negative attributes.

[0095] The system may additionally provide output identified as associated with addiction, such as gambling addiction, or a subject otherwise being 'hooked' on the game. When the level of engagement or minor addiction is viewed as acceptable, a positive weighting may be used in the training, whereas when the addiction is viewed as unacceptable or excessive, a negative weighting may be used in the training.

[0096] The artificial intelligence, machine learning, neural network, use of user response in training AI/ML systems (generally FIG. **11** and discussion, above), may advantageously be utilized in game design and develop, entertainment development and/or any creative developmental effort.

[0097] The systems may constitute a matrix of tools. They may comprise a given set of tools. In a more fundamental way, they comprise a tool to discover the tools. Tools may he game states, entertainment states or any form of state or matter.

[0098] The following will be described as to game development, but the tools, systems, methods and architectures may be applied to entertainment or any creative effort. As to a particular game, a first option is to provide only basic rules of that given game. The system may play against itself, or alternatively, play against other systems, in order to discovery winning game play strategies. In yet another option, the system may be provided with known gambits, with the system permitted to use or ignore the gambits. In yet an alternative embodiment, the system may be provided with a library of games. The system may analyze the library of games for game elements, game mechanics or core loops. Optionally, the system may limit analysis of the library of games to similar games, or may consider all games, optionally divided into subunits, e.g. card games, board games, video games. Once the various core loops or game elements are defined, the system may combine them in various combinations and permutations so as to define a new game or game play sequence. The system may recognize patterns in the data. Values may be assigned to decisions at various points or game states or game state decision points. The use of user response may be advantageously used in game formation and optimization. The use of user response is particularly suited to reinforced learning.

[0099] The system may operate in a hierarchical manner. Hierarchical systems may be used, where it may vary a 'subservient' mandated parameter so long as 'superior' or 'master' mandated parameter is met. By way of example, a 'super' mandated parameter' may be used to guarantee a particular outcome. Alternatively, an administrative control may be granted, such as to set a 'top level' constraint.

[0100] The system may consider separate functions in a cooperative action. Functions may be reassigned or moved to other, especially lower, levels of action. The system may provide new variables. By providing a hierarchical response, core functionality may be maintained. Optionally, the system may employ a "kill switch" for the system, an apoptosis, such as based on a command such as from an administrator, or based on predefined criteria.. The system may provide a package of experience r Total Recall') such as in a continuous, state and/or persistent state.

[0101] FIGS. **12 & 13** relate to various dynamic, that is changeable, systems. In the designation "d-API" and "d-SDK", 'd' stands for 'dynamic' and is capable of change within and by the system. The format of the interaction (request and/or response) may be changes. Alternately, it may change the type, quantity or quality of information provided in the response. Other factors that may be changed include the ability of the request to alter the information via the API or SDK. Changes may be made to other operational or administrative rights or permissions, such as read only access, read and write, edit rights, super administrative rights. These provide for dynamic change under adaptive control.

[0102] Within the dynamic-Application Programming Interface (d-API), an initial format for request and response is defined, this may be considered in an 'if-then' statement: IF you ask for X in an agreed upon format, THEN system will provide X. The dynamic system may vary the format, and/or response. An intelligent dynamic update may be based on Al, machine learning or analytics. While not limited to the following, some or all of these changes may be implemented dynamically: the format of the interaction (request and/or response), access to more information or functionality, e.g. read only, or modification rights, the ability to provide information or data to the system, and the ability to change data.

[0103] Within the dynamic Game Development Kit (d-GDK), an initial kit is provided. The system then permits dynamic modification of the GDK. Preferably, dynamic modification is based on AI or Machine Learning or analytics.

[0104] Dynamic Segregated Lottery (d-SL) may be provided wherein one or more functional units or the lottery may be provided. A virtualized system may be utilized, such as in the use of a virtualized server.

[0105] FIGS. **14-20** relate to a blockchain implementation for games, entertainment or other useful ends. Blockchain uses a cryptographic 'hash' to identifies each block and transaction. Each successive block contains a hash of the previous code. This permanently fixes transactions in chronological order. The blockchain utilizes both a private key and public key. The prior hash is added to the new blockchain with a nonce to form a new hash,

[0106] Cryptocurrency provides for cryptographically secure transact ons Cryptocurrency is a programmable currency or decentralized value transfer system. It is also a decentralized virtual currency or decentralized digital currency.

[0107] Proof of work, or proof of stake, is the "right" to participate in the blockchain. It must be onerous enough to prevent changes without redoing the work. Bitcoin is a created currency which is mined and serves as a reward for payment processing work, Blockchain cryptocurrency involves no transaction charges or fees paid by purchaser. There are no refund rights or chargebacks.

[0108] It may be implemented in any form of network, both public and private, Open software and proprietary software may be used. Storage may be local storage or cloud storage and computing. Analytics may be performed locally or in a cloud analytics system. Analytics As A Service (AAAS) may be performed. Systems may be permissioned v. permission less distributed systems.

[0109] FIGS. **21** through **23** relate to smart contracts. The core elements are, first, a set of promises which may be contractual or non-contractual. Second, they are specified in digital form, operate electronically, where the contractual clauses or functional outcomes embedded in code. Third, they include protocols, or technology enabled rules-based operations. Fourth, the parties perform on the promises through automated performance, in a generally irrevocable manner.

[0110] Smart contracts automate different processes and operations,.In one embodiment, they automate "if-this-then-that" on self-executing basis with finality. They may provide for payments. Actions may be conditioned on a payment or payments, such as with the control of collateral based on payment.

[0111] Smart contracts may be implemented via blockchain. This forms a trusted system, which may be implemented in a business to business implementation (B to B) and/or peer-to-peer implementation. The machine-to-machine implementation permits various combinations. In one implementation, a blockchain is combined with devices comprising the Internet of Things (IoT). In yet another combination, the blockchain may be combined with devices comprising the Internet of Things in combination with artificial intelligence. Generally, the block contains smart contract program logic. It bundles together the messages relating to a particular smart contract including inputs, outputs, and logic. In yet another implementation, they may provide contracts for difference, such as in use the current market price to adjust balances and disperse cash flow.

[0112] Smart contracts are a trust shifting technology. They reduce counter-party risk. Preferably, this serves to increase credit.

[0113] Smart contracts rosy be implemented in various models. They may be a contract entirely in code. They may be a contract in code with separate natural language version. They may be split natural language contract with encoded performance. Alternatively, they may be a natural language contract with encoded payment mechanism.

[0114] Smart contract initiation involves a consensus. An algorithm constitutes a set of rules for how each participant in the contract processes messages. They may be implemented in a permission-less manner, wherein anyone may submit messages for processing. The submitter may be involved in consensus. Alternately, they may delegate decision making such as to an administrator or sub-,group of participants. An alternative implementation is to have a permissioned system, in which the participants are limited. They are generally pre-selected. They are then subject to gated entry and be subject to the satisfaction of certain requirements and/or approval of an administrator.

[0115] Smart contracts are subject to various methods of formation. They may by agreement such as where there is a common cooperative opportunity or a defined desired outcome. These may include business practices, asset swaps, and transfer of rights. Next, conditions set for initiation of the contract. That may be by the parties themselves, or by the occurrence of some external event, such as time, other quantifiable measure or location. Typically, they generate a code, which is encrypted and chained with blockchain technology. It may be authenticated and verified. Upon execution and processing, the network updates all ledgers to indicate current state. Once verified and posted, they cannot be changed, with only additional blocks, appended.

[0116] To restate, the smart contract serves as a distributed application on networks with independent built-in trust mechanisms. The program is entrusted with the unit of value combined with rules for transfer of ownership of the unit of value. They serve as self-executing programs that automatically fulfill the terms of a programmed relationship.

[0117] FIG. **20** shows a Lottery embodiment implemented as a smart contract. The method for implementing a lottery includes the following steps. A time frame is set in which to receive cryptocurrency. Second, cryptocurrency is received with owner identification within the timeframe. The window opens for a specified duration, afterwards at which the window closes. The smart contract generates or receives a random event, such as from a random number generator. The random number generator should include an algorithmic guarantee of randomness and a guarantee of no hack. The contract selects a new owner (winner) among the owner identification related cryptocurrencies. It then assigns new ownership of cryptocurrency to selected new owner (winner).

[0118] Smart contracts may be used to implement a core loop or a game mechanic. The following core loops and game mechanics comprise a partial list of those that may be implemented, including but not limited to JACKO, POKO, Hot Seat, Hi Lo, Rock, Paper, Scissors. In the Zone and iLotto or other array or geography based game mechanics or core loops. Any subunit of the game mechanic or core loop may itself be used as a game mechanic or core loop.

[0119] Jacko is a game comprising the steps of: randomly selecting a target number from a first range of numbers having a minimum, and maximum number, presenting an indication of the target number to the player, selecting a number for the player, the number being selected from a second range, having a minimum and maximum, where the maximum is equal to or less than ½ of the minimum of the first range, receiving an indication from the player whether to draw again, and if so, randomly selecting a number from the second range, accumulating the total of the player's draws, and repeating this step until either the player declines to draw or the total exceeds the target number, and in the event the player declines to draw, randomly selecting numbers from the second range, accumulating those numbers, comparing them to the player's accumulated amount, and assigning as to the winner whomever has a total closest to, but not exceeding, the target.

[0120] Poko is a multi-player game where multiple indicia are awarded a predefined value, where other players have no information as to at least some of the indicia held by other players.

[0121] High Lo is a game comprising the steps of: performing a first lottery selection of a series of randomly drawn numbers, receiving from a player an indication whether the next randomly drawn number will be higher or lower than the preceding number, and if correct, awarding winnings correlated to the amount of the randomly drawn number, and continuing until the player fails to predict the high/low outcome, or elects to stop.

[0122] In the Zone is a game of chance comprising the steps of randomly selecting a player's target number within a predefined range of numbers, the range having a minimum and a maximum, randomly selecting a series of numbers for use in a lottery game, the minimum of the predefined range of numbers being at least equal to the sum of the lowest possible total for the series of the lowest possible total for the series of numbers and the maximum of the predefined range of numbers, totaling the random selected series of numbers through the conclusion of the selection, and assigning prize amounts to players having a player's number not exceeding the total based upon the proximity of the player's number and the total number,

[0123] Rock Paper Scissors is a game with three or more options having an assigned priority of options relative to one another.

[0124] Hot Seat is a game of increasing risk/reward including the ability to 'opt out' in Smart Contract. A method for game play in a multi-level game of chance culminating in a final level, comprises the steps of presenting, at a given level, a plurality of random options wherein at least one option is a positive option, another option is a negative option, and a third option requiring a further decision, receiving a selection regarding which one of the plurality of random option is selected, and if the positive option was selected, cumulating the positive option result with the prior positive option results, but if the negative option was selected, cumulating the negative option result, comparing the cumulative result with a predetermined number, and replaying the same level if the cumulative number is less than the predetermined number or terminating the game if the cumulative number equals the predetermined number, and if the third option was selected, receiving a selection regarding the decision, respecting the above steps until the player stops, the predetermined number of negative events occurring or the final level is related.

[0125] iLotto is a grid or geography based system including a display for presenting a grid of identifying objects, an input for receiving a player selection of an identifying object, a random generator for randomly selecting a winning identifying object, and a point tally system for awarding points to the player according to the rules comprising a first point value if the player selected identifying object exactly matches the winning identifying object, a second point value if the player selected identifying object is in a geometric relationship with the winning identifying object, and a third, negative, point value if the player is not awarded the first point value or the second point value.

[0126] FIG. **23** relates to implementation of mandated and variable parameters. Mandated parameters are set in smart contracts. Examples of mandated parameters include payout percentage and payout amount. Variable parameters are subject to mandated parameters, providing entertainment options.

[0127] FIG. **24** depicts a wallet serving for the electronic storage of cryptocumency. This represents a graphical user interface ("GUI"), such as on a phone or computer display. Various forms of cryptocurrency may be displayed on the GUI and stored in the wallet. Points may be awarded, such as for loyalty, frequency and airtimes. Recent or latest transactions may be listed, indicating the date, purpose and amount. A total account value may be shown.

[0128] Cryptocurrency systems and smart contracts may be implemented in combination with other systems. One additional system comprises a frequent user or player's club system. They may be combined with other forms of 'currency lite', including micro-transactions and micro-payments. They may be used in combinations with smart properties, that is digital assets or physical things that know who their owner is. Digital assets are anything that exists in digital, typically binary, format and comes with the right to use. Examples include images, including still pictures and video or dynamic images, audible content, such as sounds, music or performances, and digital documents. Property whose ownership is controlled via distributed trusted network, e.g., blockchain using contracts. They may be further used in combination with geolocation, wherein the physical location (geolocation) of various components and architectural components are optionally a component of the system. Limits may be placed on the geography of game play. The system can ensure compliance with geolocation of data routing.

[0129] FIGS. **25** through **27** relate to systems having segregated secure functions and public functions. This provides a secure platform with multiple interfaces to public functions and public entities. The segregated secure functions provide the function of the trusted agent. The secure functions include one or more of the following. First, outcome determination. This may include the use of a random number generator (RNG) or probability engine. Second, user or player account information is stored. Third, monetary accounting or transactions are stored. Fourth, regulatory and compliance interface is performed. Fifth, interfaces such as a developer interface. Sixth, regulatory functions including Q&A testing, compliance, testing and approval may be provided.

[0130] The public functions include some or all of the following. First, the public system issues a 'call' to the secure system. A 'call' may be via an Application Programming interface (API) or d-API. The "OPEN" system call makes calls to secure system for secure data. Second, a designer interface serves to access tools, APIs, a Development Kit (DK), and a Software Development Kit (SDK). Third, a marketplace interface serves as a lottery interface and optionally an application or app store. Fourth, an operator interface serves to interface with an operator or organizer, e.g., a charity. It preferably serves to publish, market, and sell. Fifth, the user interface permits registration, play activity and persistent history.

[0131] The system components may vary by function. Public interfaces and functions preferably comprise an "open" platform. This allows for arbitration and agreement with the secure entity regarding game operations to be performed by the secure entity, eg., payout %; vGLEPs, who may play, and geolocation. The secure entity performs secure functions including game outcomes, financial matters and secure user data. The end users utilize a "channel mix", including but not limited to web, mobile app, mobile web, tablet, computer, display enabled Devices (wireless), touch screen equipment at retailer, e,g., countertop games. The private entity may impose rate limits and impose responsible gaming controls.

[0132] FIGS. **28** and **29** describe hybrid and hierarchical systems. A centralized system, such as a state run lottery may be combined with a decentralized system, such as a blockchain implementation. Hierarchical order may be imposed within the system. In a system using mandated and variable parameters, a hierarchy of mandated parameters may be established, and then various variable parameters may be subject to the appropriate mandated parameter. In another application, a global use rate limit may be imposed at a high level in the hierarchy. Hierarchical use rate limits may be imposed. Various topologies of systems include master slave, master over multiple slaves and circular systems.

[0133] FIG. **30** relates to a game or lottery linked credit card and credit card function. A credit card and credit functionality may be linked to lottery or other game play. Through use of the credit card, a conversion rate is established. By way of example, for every $100 of purchases, $1 in lottery play is made. The rate may be variable, such as based upon institution. In the event a charitable organization organized or sponsored the lottery or game, every $100 of purchases accrues $2 for the organization. A split may also be performed, such as for every $100 of purchases accrues $1 in the lottery or game for the credit card owner and $1 for the organization.

[0134] In alternative embodiments, the mobile gaming device may be connected to the gaming machine with a cable, either directly connected to a port of the gaming machine or via a network communicating with the gaming machine.

[0135] The software used to program the gaming machines and servers in accordance with the embodiments described herein may be initially stored on a ROM, such as a CD or an electronic memory device. Such CDs and devices are non-transitory computer readable mediums having the appropriate computer instructions stored thereon. The programming may also be downloaded to the gaming machines via the casino's network.

[0136] It should be appreciated that the terminals, processors, or computers described herein may be embodied in any of a number of forms, such as a rack-mounted computer, a desktop computer, a laptop computer, or a tablet computer. Additionally, a computer may be embedded in a device perhaps not generally regarded as a computer but with suitable processing capabilities, including an electronic gaming machine, a Web TV, a Personal Digital Assistant (PDA), a smart phone or any other suitable portable or fixed electronic devices.

[0137] Also, a computer may have one or more input and output devices. These devices can be used, among other things, to present a user interface. Examples of output devices that can be used to provide a user interface include printers or display screens for visual presentation of output and speakers or other sound generating devices for audible presentation of output. Examples of input devices that can be used for a user interface include keyboards, and pointing devices, such as mice, touch pads, and digitizing tablets. As another example, a computer may receive input information through speech recognition or in other audible formats.

[0138] Such computers may be interconnected by one or more networks in any suitable form, including as a local area network or a wide area network, such as an enterprise network or the Internet. Such networks may be based on any suitable technology and may operate according to any suitable protocol and may include wireless networks, wired networks or fiber optic networks. As used herein, the term "online" refers to such networked systems, including computers networked using, e.g. dedicated lines, telephone lines, cable or ISDN lines as well as wireless transmissions. Online systems include remote computers using, e.g., a local area network (LAN), a wide area network (WAN), the Internet, as well as various combinations of the foregoing. Suitable user devices may connect to a network for instance, any computing device that is capable of communicating over a network, such as a desktop, laptop or notebook computer, a mobile station or terminal, an entertainment appliance, a set-top box in communication with a display device, a. wireless device such as a phone or smartphone a game console, etc. The term "online gaming" refers to those systems and methods that make use of such a network to allow a game player to make use of and engage in gaming activity through networked, or online systems, both remote and local. For instance, "online gaming" includes gaming activity that is made available through a website on a the Internet.

[0139] Also, the various methods or processes outlined herein may be coded as software that is executable on one or more processors that employ any one of a variety of operating systems or platforms. Additionally, such software may be written using any of a number of suitable programming languages and/or programming or scripting tools, and also may be compiled as executable machine language code or intermediate code that is executed on a framework or virtual machine.

[0140] In this respect, embodiments may provide a tangible, non-transitory computer readable storage medium (or multiple computer readable storage media) (e.g., a computer memory, one or more floppy discs, compact discs (CD), optical discs, digital video disks (DVD), magnetic tapes, flash memories, circuit configurations in Field Programmable Gate Arrays or other semiconductor devices, or other non-transitory, tangible computer-readable storage media) encoded with one or more programs that, when executed on one or more computers or other processors, perform methods that implement the various embodiments discussed above. The computer readable medium or media can be transportable, such that the program or programs stored thereon can he loaded onto one or more different computers or other processors to implement various aspects as discussed above. As used herein, the term "non-transitory computer-readable storage medium" encompasses only a computer-readable medium that can be considered to be an article of manufacture or a machine and excludes transitory signals.

[0141] The terms "program" or "software" are used herein in a generic sense to refer to any type of computer code or set of computer-executable instructions that can be employed to program a computer or other processor to implement various aspects of, as discussed above. Additionally, it should he appreciated that according, to one aspect of this embodiment, one or more computer programs that when executed perform methods need not reside on a single computer or processor, but may be distributed in a modular fashion amongst a number of different computers or processors to implement various aspects of embodiments described herein.

[0142] Computer-executable instructions may be in many forms, such as program modules, executed by one or more computers or other devices. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Typically the functionality of the program modules may be combined or distributed as desired in various embodiments.

[0143] Also, data structures may be stored in computer-readable media in any suitable form. For simplicity of illustration, data structures may be shown to have fields that are related through location in the data structure. Such relationships may likewise be achieved by assigning storage for the fields with locations in a computer-readable medium that conveys relationship between the fields. However, any suitable mechanism may be used to establish a relationship between information in fields of a data structure, including through the use of pointers tags, addresses or other mechanisms that establish relationship between data elements.

[0144] Various aspects of embodiments described herein may be used alone, in combination, or in a variety of arrangements not specifically discussed in the embodiments described in the foregoing and the concepts described herein are therefore not limited in, their application to the details and arrangement of components set forth in the foregoing description or illustrated in the drawings. For example, aspects described in one embodiment may be combined in any manner with aspects described in other embodiments.

[0145] Also, embodiments described herein may provide a method, of which an example has been provided. The acts performed as part of the method may be ordered in any suitable way. Accordingly, embodiments may be constructed in which acts are performed in an order different than illustrated, which may include performing some acts simultaneously, even though shown as sequential acts in illustrative embodiments.

[0146] While embodiments have been described with reference to certain exemplary features thereof, those skilled in the art may make various modifications to the described embodiments. The terms and descriptions used herein are set forth by way of illustration only and not meant as limitations. In particular, although embodiments have been described by way of examples, a variety of devices would practice the inventive concepts described herein. Embodiments have been described and disclosed in various terms, the scope of the embodiments is not intended to be, nor should it be deemed to be, limited thereby and such other modifications or embodiments as may be suggested by the teachings herein are particularly reserved, especially as they fall within the breadth and scope of the claims here appended. Those skilled in the art will recognize that these and other variations are possible as defined in the following claims and their equivalents. Although the foregoing invention has been described in some detail by way of illustration and example for purposes of clarity and understanding, it may be readily apparent to those of ordinary skill in the art in light of the teachings of this invention that certain changes and modifications may be made thereto without departing from the spirit or scope of the appended claims.

[0147] All publications and patents cited in this specification are herein incorporated by reference as if each individual publication or patent were specifically and individually indicated to be incorporated by reference in their entirety.

REFERENCES

[0148] ARM, IBM, "The Internet of Things Business Index 2017, Transformation In Motion", The Economist, Intelligence Unit Limited 2017, pages 1-22.

[0149] Crosby, et al., "Blockchain Technology: Beyond Bitcoin", Applied Innovation Review, Issue No. 2, Sutardja Center for Entrepreneurship & Technology, Berkeley Engineering, June 2016, pages 119.

[0150] Fisher, "Decentralized Peer to Peer Game Assets Platform, Integration with Third Party Games using Smart Contract," Aug. 4, 2014, 12 pages,

[0151] Hinton et al., "A Fast Learning Algorithm For Deep Belief Nets", Neural Computation, 18, 1527-1554, 2006.

[0152] Jouppi, et al,, "In-Datacenter Performance Analysis of a Tensor Processing Unit™", To appear at the 44th International Symposium on Computer Architecture (ISCA), Toronto, Canada, Jun. 26, 2017, pages 1-17.

[0153] LeCun, et al., "Deep Learning", Nature, Vol. 521, 28 May 2015, pages 436-444,

[0154] Marvin, "Blockchain A- Z: Everything You Need to Know About the Game-Changing Tech Beneath Bitcoin", Jun. 3, 2016, 9 pages.

[0155] Marvin, "Blockchain: The Invisible Technology That's Changing the World", Feb. 6, 2017, 32 pages.

[0156] Mougayar, The Business Blockchain, pages 6-9, 128-133, 2016, published by John Wiley & Sons, Hoboken, N.J.

[0157] Nakamoto, "Bitcoin—A Peer to Peer Electronic Cash System", 2008, pages. 1-9.

[0158] Ng, "What Artificial Intelligence Can and Can't Do Right Now", Harvard Business Review, Nov. 9, 2016, 5 pages.

[0159] O'Dowd, et al., "IBM's Open. Blockchain, Making Blockchain Real for Enterprises", IBM Blockchain April 2016, pages 1-20.

[0160] Ronan, "Deep Learning predicts Toto Numbers", Academy of Paris, Apr. 1, 2016, pages 1-4.

[0161] Smart Contract Alliance, "Smart Contracts: 12 Use Cases for Business and Beyond, A Technology, Legal & Regulatory information, prepared by Smart Contracts Alliance—in collaboration with Deloitte. An industry initiative of the Chamber of Digital Commerce", December 2016, pages 1-53.

[0162] Turing, "Computing Machinery and Intelligence", Mind 49: 1950, pages 433-460,,

[0163] Wood, "Ethereum: A Secure Decentralized Generalized Transaction Ledger", Homestead Draft, 2014, pages 1-32.

[0164] Wu, et al, "Google's Neural Machine Translation System: Bridging the Gap between Human and Machine Translation", 8 Oct. 2016, pages 1-23,

[0165] Yli-Huumo, et al., "Where is Current Research on Blockchain Technology? A Systematic Review", Oct. 3, 2016, pages 1-27.

GLOSSARY

[0166] 51% Attack: An attack on the Bitcoin network which allows the attacker to create fraudulent transactions, see Double Spend. This is possible because controlling more than 50% of the Bitcoin network's hash rate means the attacker can out-compute everyone else who is mining.

A

[0167] Account: Accounts have an intrinsic balance and transaction count maintained as part of the Ethereum state. They also have some (possibly empty) EVM Code and a (possibly empty) Storage State associated with them. Though homogenous, it makes sense to distinguish between two practical types of account: those with empty associated EVM Code (thus the account balance is controlled, if at all, by sonic external entity) and those with non-empty associated EVM Code (thus the account represents an Autonomous Object). Each Account has a single Address that identifies it.

[0168] Address: A bitcoin address is used to receive and send transactions on the bitcoin network, it contains a string of alphanumeric characters, but can also be represented as a scannable OR code. A bitcoin address is also the public key in the pair of keys used by bitcoin holders to digitally sign transactions (see Public Key).

[0169] Address; A code e.g., a 160-bit code, used for identifying Accounts,.

[0170] Agreement Ledger: An agreement ledger is distributed ledger used by two or more parties to negotiate and reach agreement.

[0171] Airdrop: A method of distributing cryptocurrency amongst a population, first attempted with Auroracoin (auroracoin) in early 2014.

[0172] Algorithm: A process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer.

[0173] Altcoin: The collective name for cryptocurrencies offered as alternatives to bitcoin. Litecoin, Feathercoin and PPcoin are all altcoins.

[0174] AML: Anti-Money Laundering techniques are used to stop people corverting illegally of funds, to appear its though they have been earned, AML mechanisms can be legal or technical in nature Regulators frequently apply AML techniques to bitcoin exchanges,

[0175] App: An end-user-visible application, e.g., hosted in the Ethereum Browser.

[0176] Application Program Interface (API): A specification used as an interface by components, often software components, to communicate with one another. May include specifications for routines, data structures, object classes, and variables.

[0177] Arbitrage: The generation of risk free profits by trading between markets which have different prices for the same asset.

[0178] ASIC: An Application Specific Integrated Circuit is a silicon chip specifically designed to do a single task. In the case of bitcoin, they are designed to process SHA-256 hashing problems to mine new bitcoins.

[0179] ASIC Miner: A piece of equipment containing an ASIC chip, configured to mine for bitcoins. They can come in the form of boards that plug into a backplane, devices with a USB connector, or standalone devices including all of the necessary software, that connect to a network via a wireless link or ethernet cable.

[0180] ASIC Mining: Many miners purchase separate computing devices set aside solely for mining. As an alternative, they can also get an Application Specific integrated Circuit (ASIC); this is a specially-designed computer chip created to perform one specific function, and only that function—in this case, mining calculations. ASICs reduce the processing power and energy required for mining, and can help reduce the overall cost of the process in that way. Whether the. ASIC—a term that refers to the specialized chip itself—is integrated into an existing computing system, or functions as a stand-alone device, the term "ASIC" is often used generically to refer to the overall system itself, and not just the chip.

[0181] Asymmetric Key Algorithm: This is the algorithm used to generate public and private keys, the unique codes that are essential to cryptocurrency transactions. In a symmetric key algorithm, both the sender and receiver have the same key; they can encrypt and exchange information privately, but since both parties have the decoding information, they can't keep information private from one another. With an asymmetric key algorithm, both parties have access to the public key, but only the person with the private key can decode the encryption; this assures that only they can receive the funds.

[0182] Attestation Ledger: A distributed ledger providing a durable record of agreements, commitments or statements, providing evidence (attestation) that these agreements, commitments or statements were made.

[0183] Autonomous eras: Software that makes decisions and acts on them without human intervention.

[0184] Autonomous Object: A notional object existent only within the hypothetical state of Ethereum. Has an intrinsic address and thus an associated account; the account will have non-empty associated EVM Code, incorporated only as the Storage State of that account.

B

[0185] Base58; Base58 encodes binary data into text and is used to encode Bitcoin addresses. Created by Satoshi Nakamoto, its alphanumeric characters exclude "0". "O", "1", "I" since they are hard to distinguish.

[0186] Bases Check: A variant of Base58 used to detect typing errors in bitcoin addresses.

[0187] BIP: An acronym for "Bitcoin Improvement Proposals" which can be submitted by anyone who wants to improve the Bitcoin network.

[0188] Bit: Name of a Bitcoin denomination equal to 100 satoshis (1 millionth of 1 BTC). In 2014 several companies including Bitpay and Coinbase, and various wallet apps adopted bit to display bitcoin amounts.

[0189] Bitcoin (uppercase): The well know cryptocurrency, based on the proof-of-work blockchain.

[0190] bitcoin (lowercase): The specific collection of technologies used by Bitcoin's ledger, a particular solution. Note that the currency is itself one of these technologies, as it provides the miners with the incentive to mine.

[0191] Bitcoin (unit of currency): 100,000,000 satoshis. A unit of the decentralized, digital currency which can be traded for goods and services. Bitcoin also functions as a reserve currency for the altcoin ecosystem.

[0192] Bitcoin 2.0: A reference word for applications of bitroin or Blockchain technology that is more advanced or complicated than the basic payment system application proposed by the Bitcoin white paper. Examples of Bitcoin 2.0 projects include Counterparty, Ethereum, Blockstream, Swarm, Domus and Hedgy.

[0193] Bitcoin ATM: A bitcoin ATM is a physical machine that allows a customer to buy bitcoin with cash. There are many manufacturers, some of which enable users to sell bitcoin for cash. They are also sometimes called 'BTMs' or 'Bitcoin AVMS'. CoinDesk maintains a worldwide map of operational bitcoin ATM machines and a list of manufacturers.

[0194] Bitcoin Core: New name of Bitcoin QT since release of version 0.9 on Mar. 19, 2014. Not to confuse with CoreBitcoin, a Objective-C implementation published in August 2013.

[0195] Bitcoind: Original implementation of Bitcoin with a command line interface. Currently a part of BitcoinQT project. "D" stands for "daemon" per UNIX tradition to name processes running in background.

[0196] Bitcoin Days Destroyed: An estimate for the "velocity of money" with the Bitcoin network. This is used because it gives greater weight to bitcoins that have not been spent for a long time, and better represents the level of economic activity taking place with bitcoin than total transaction volume per day.

[0197] Bitcoin Investment Trust: This private, open-ended trust invests exclusively in bitcoins and uses a state-of-the-art protocol to store them safely on behalf of its shareholders. It provides a way for people to invest in bitcoin without having to purchase and safely store the digital currency themselves.

[0198] Bitcoinj: A Jaya implementation of a full Bitcoin node by Mike Hearn. Also includes SPV implementation among other features.

[0199] BitcoinJS: An online library of javascript code used for Bitcoin development, particularly web wallets. bitcoinjs.org(http://bitcoinjs.org)

[0200] Bitcoin Market Potential Index (BMPI): The Bitcoin Market Potential index (BMPI) uses a data set to rank the potential utility of bitcoin across 177 countries. It attempts to show which markets have the greatest potential for bitcoin adoption.

[0201] Bitcoin Network: The decentralized, peer-to-peer network which maintains the blockchain. This is what processes all Bitcoin transactions.

[0202] Bitcoin Price Index (BPI): The CoinDesk Bitcoin Price Index represents an average of bitcoin prices across leading global exchanges that meet criteria specified by the BPI. There is also an API for developers to use.

[0203] Bitcoin Protocol: The open source, cryptographic protocol which operates on the Bitcoin network., setting the "rules" for how the network runs.

[0204] BitcoinQT: Bitcoin QT is an open source software client used by your computer. It contains a copy of the blockchain and once installed it turns your computer into a node in the Bitcoin Network. Also acts as a "desktop wallet."

[0205] Bitcoin-ruby: A Bitcoin utilities library in Ruby by Julian Langschaedel. Used in production on Coinbase.com

[0206] Bitcoin Sentiment Index (BSI): The Bitcoin Sentiment Index is a measure of whether individuals feel the digital currency's prospects are increasing or decreasing on any given day, and is powered by data collected by Qriously.

[0207] Bitcoin Whitepaper: The bitcoin whitepaper was written by 'Satoshi Nakamoto' and posted to a Cryptography Mailing list in 2008. The paper describes the bitcoin protocol in detail, Satoshi Nakamoto followed this by releasing the bitcoin code in 2009.

[0208] Bitcoin white paper: In November 2008, a paper, authored (probably pseudonymously) by Satoshi Nakamoto, was posted on the newly created Bitcoin.org website with the title 'Bitcoin; A Peer-to-Peer Electronic Cash System'. The eight-page document described methods of using a peer-to-peer network to generate "a system for electronic transactions without relying on trust" and laid down the working principles of the cryptocurrency.

[0209] Bitcore: A Bitcoin toolkit by Bitpay written in javaScript. More complete than Bitcoinjs.

[0210] BitPay: A payment processor for bitcoins, which works with merchants, enabling them to take bitcoins as payment.

[0211] BitStamp: An exchange for bitcoins that has been gaining in popularity.

[0212] Block: This is a collection of transaction data, one of the fundamental elements of cryptocurrency. As transactions are made, the pertinent information for each one is collected, and when the gathered data reaches a predetermined size, it's bundled up as a block. As soon as possible after blocks are created, they're processed by investors for transaction verification; this process is known, as mining.

[0213] Blockchain: The full list of blocks that have been mined since the beginning of the bitcoin cryptocurrency. The blockchain is designed so that each block contains a hash drawing on the blocks that came before it. This is designed to make it more tamperproof. To add further confusion, there is a company called Blockchain, which has a very popular blockchain explorer and bitcoin wallet.

[0214] Block Halving: [see Halving], The halving of the bitcoin reward that miners receive for mining a block. This takes place approximately every 4 years (every 210,000 block to be precise).

[0215] Block Header: Contains information about a block, such as the hash of the previous block header, its version number, the current target, a timestamp, and a nonce.

[0216] Block Height: Block height refers to the number of blocks connected together in the block chain. For example, Height **0**, would be the very first block, which is also called the Genesis Block.

[0217] Blockchain.info: A web service running a Bitcoin node and displaying statistics and raw data of all the transactions and blocks. It also provides a web wallet functionality with lightweight clients for Android, iOS and OS X.

[0218] Block Reward: The reward given to a miner which has successfully hashed a transaction block. This can be a mixture of coins and transaction fees, depending on the policy used by the cryptocurrency in question, and whether all of the coins have already been successfully mined. Bitcoin currently awards 25 bitcoins for each block. The block reward halves when a certain number of blocks have been mined. In bitcoin's case, the threshold is every 210,000 blocks.

[0219] Bootstrapping: Technique for uploading the program onto a volunteer's computer or mobile device through a few simple instructions that set thee rest of the program in motion.

[0220] Trading: Software programs that operate on trading platforms, executing buy and sell orders with pre-programmed trading instructions.

[0221] Brain Wallet: [see Wallet] A bitcoin wallet which uses a long string of words to secure its coins. This "passphrase" can be memorized, allowing the wallet owner to spend bitcoins by simply remembering the passphrase.

[0222] Brainwallet.org: Utility based on bitcoin to craft transactions by hand, convert private keys to addresses and work with a brain wallet.

[0223] BTC: The short currency abbreviation for bitcoins.

[0224] Buy Order: A buy order is established when an investor approaches an exchange and wants to purchase cryptocurrency. These can range from very simple orders ("I want to spend x amount of dollars on Bitcoins") to complex ones that include factors such as time frame in which the order should be filled, range of price, and so forth. Most exchanges allow for these to he entered online, but some investors prefer to go over the derails directly with an exchange representative. Buy orders don't necessarily guarantee your purchase; if your price is too low, for example, the offer may expire without being filled unless you make adjustments.

C

[0225] Capital Controls: These are local measures such as transaction taxes, limits, or other prohibitions that a government can use to regulate flows from capital markets into and out of the country.

[0226] Casascius Coins: Physical collectible Coins produced by Mike Caldwell. Each coin contains a private key under a tamper-evident hologram. The name "Casascius" is formed from a phrase "call a spade a spade", as a response to a name of Bitcoin itself.

[0227] Central Ledger: A central ledger refers to a ledger maintained by a central agency.

[0228] Change: Informal name for a portion of a transaction output that is returned to a sender as a "change" after spending that output. Since transaction outputs cannot be partially spent, one can spend 1 BTC out of 3 BTC output only be creating two new outputs: a "payment" output with 1 BTC sent to a payee address, and a "charge" output with remaining 2 BTC (minus transaction fees) sent to the payer's addresses. BitcoinQT always uses new address from a key pool for a better privacy. Blockchain.info sends to a default address in the wallet. A common mistake when working with a paper wallet or a brain wallet is to make a change transaction to a different address and then accidentally delete it. E.g. when importing a private key in a temporary Bitcoin QT wallet, making a transaction and then deleting the temporary wallet.

[0229] Checkpoint: A hash of a block before which the BitcoinQT client downloads blocks without verifying digital signatures for performance reasons. A checkpoint usually refers to a very deep block (at least several days old) when it is clear to everyone that the block is accepted by the overwhelming majority of users and reorganization with not happen past that point. It also helps protecting most of the history from a 51% attack, Since checkpoints affect how the main chain is determined, they are part of the protocol and must be recognized by alternative clients (although the risk of reorganization past the checkpoint would be incredibly low).

[0230] Circle: Circle is an exchange and wallet service, offering users worldwide the chance to store, send, receive and exchange bitcoins.

[0231] Client: A software program running on a desktop or laptop computer, or mobile device. It connects to the bitcoin network and forwards transactions. It may also include a bitcoin wallet (see Node).

[0232] Cloud: A reference to the Internet and functions it can carry out for anyone such as storage, file sending, and using apps.

[0233] Cloud-hashing/mining: A type of mining where people can pay to rent computer power from someone else in the cloud to mine bitcoin or other cryptocurrencies. This is done by selling mining contracts. Cloudhashing is also the name of a business which offers this service.

[0234] Coin: An informal term that means either 1 bitcoin, or an unspent transaction output that can be spent.

[0235] Coin Age: The age of a coin, defined as the currency amount multiplied by the holding period.

[0236] Coinbase: Another name for the input used in a bitcoin's generation transaction. When a bitcoin is mined, it doesn't come from another bitcoin user, but is generated as a reward for the miner. That reward is recorded as a transaction, but instead of another user's bitcoin address, some arbitrary data is used as the input. Coinbase is also the name of a bitcoin wallet service that also offers payment processing services for merchants and acts as an intermediary for purchasing bitcoins from exchanges.

[0237] Coinbase.com: US based Bitcoin/USD exchange and web wallet service.

[0238] Cold Storage: The safest way to store private keys is by keeping them offline in "cold storage". This could be in the form of a hardware wallet, USB stick or paper wallet. These wallets are known as "cold wallets".

[0239] Collective Mining: The commitment of resources and materials to the process of mining digital currency data blocks often proves to be too expensive for individuals to take part. As a result, many enterprising businesses have worked out a way to make mining more affordable for those miners who would otherwise be left out. These companies invest in the hardware that allows for high-end mining power, and they in turn lease the access to this mining capability to third parties. As an individual miner, this means you can sign a contract that allows you to use a predetermined amount of mining power through cloud computing, without the hassle or expense of buying or maintaining the processing power needed to do so. The block rewards that come with the successful mining of the data block go to the individual miner who purchased the contract from the collective mining company.

[0240] Colored Coins: A proposed add-on function for bitcoin that would enable bitcoin users to give them additional attributes. These attributes could be user-defined, enabling you to mark a bitcoin as a share of stock, of a physical asset. This would enable bitcoins to be traded as tokens for other property.

[0241] CompactSize: Original name of a variable-length integer format used in transaction and block serialization. Also known as "Satoshi's encoding". It uses 1, 3, 5 or 9 bytes to represent any 64-bit unsigned integer. Values lower than 253 are represented with 1 byte. bytes 253, 254 and 255 indicate 16-, 32- or 64-bit integer that follows. Smaller numbers can be presented different. In bitcoin-ruby it is called "var_int", in Bitcoinj it is Varint. BitconQT also has even more compact representation called Varint which is not compatible with CompactSize and used in block storage.

[0242] Confirmation: The act of hashing a bitcoin transaction successfully into a transaction block, and cementing its validity. A single confirmation will take around 10 minutes, which is the average length of time for a transaction block to be hashed. However, some more sensitive or larger transactions may require multiple confirmations, meaning that more blocks must be hashed and added to the blockchain after the transaction's block has been hashed. Each time another block is added to the blockchain after the transaction's block, the transaction is confirmed again.

[0243] Confirmation Number: Confirmation number is a measure of probability that transaction could be rejected from the main chain. "Zero confirmations" means that transaction is unconfirmed (not in any block yet). One confirmation means that the transaction is included in the latest block in the main chain. Two confirmations means the transaction is included in the block right before the latest one. Probability of transaction being reversed ("double spent") is diminishing exponentially with more blocks added "on top" of it.

[0244] Confirmed Transaction: Transaction that has been included in the blockchain. Probability of transaction being rejected is measured in a number of confirmations.

[0245] Consensus Point: A point—either in time, or defined in terms of a set number or volume of records to be added to the ledger where peers meet to agree the state of the ledger.

[0246] Consensus Process: The process a group of peers responsible for maintaining a distributed ledger used to reach consensus on the ledger's contents.

[0247] Contract: Informal term used to mean both a piece of EVM Code that may be associated with an Account or an Autonomous Object.

[0248] Core Developers: Programmers working on the open-source Source Code for Bitcoin. They are not formally employed by or paid by, and are not in control of, the Bitcoin Network; however, they have elevated access on the GitHub resource page for the Bitcoin Network where the main "reference" version of the Source Code is developed.

[0249] Counterfeiting: The act of imitating something in order to commit fraudulent behavior. An example of this is shopping with fake money.

[0250] CPU: Central Processing Unit—the 'brain' of a computer. In the early days, these were used to hash bitcoin transactions, but are now no longer powerful enough. They are still sometimes used to hash transactions for altcoins.

[0251] Crowdsourcing: The pooling of resources such as information or money contributed by the general population, to a goal. This is usually done online via websites where people can donate.

[0252] Cryptocurrency: A form of currency based on mathematics alone. Instead of fiat currency, which is printed, cryptocurrency is produced by solving mathematical problems based on cryptography.

[0253] Cryptography: The use of mathematics to create codes and ciphers that can be used to conceal information. Used as the basis for the mathematical problems used to verify and secure bitcoin transactions.

[0254] CSRNG: Acronym for "Cryptographically Secure Random Number Generator", used in private key generation for bitcoin wallets.

[0255] Cyberclones: Created by corporations by fracking digital world for their data.

D

[0256] DAO: An acronym for "Decentralised Autonomous Organization", a theoretical company that could exist in the cloud and carry out business according to preset algorithms, needing no human management. Also known as "DACs".

[0257] Darksend: Darksend is Darkcoin's decentralized mixing implementation, which was designed to give users of Darkcoin greater transactional privacy/anonymity.

[0258] DDoS: A distributed denial of service attack uses large numbers of computers under an attacker's control to drain the resources of a central target. They often send small amounts of network traffic across the Internet to tie up computing and bandwidth resources at the target, which prevents it from providing services to legitimate users, Bitcoin exchanges have sometimes been hit with DDoS attacks.

[0259] Deepweb: The content online not indexed by search engines making it difficult to access. The majority of content on the Internet resides on the deepweb and can be accessed using a program called TOR.

[0260] Demurrage: Certain currencies penalize users for hoarding, this is done via demurrage, where a fee is charged for holding Unspent coins. This fee increases as time passes.

[0261] Denial of Service [DoS]: Is a form of attack on the network. Bitcoin nodes punish certain behavior of other nodes by banning their IP addresses for 24 hours to avoid DoS. Also, some theoretical attacks like 51% attack may be used for network-wide DoS.

[0262] Depth: Depth refers to a place in the blockchain. A transaction with 6 confirmations can also be called "6 blocks deep".

[0263] Desktop Wallet: A wallet that stores the private keys on your computer, which allow the spending and management of your bitcoins.

[0264] Deterministic Wallet: A wallet based on a system of deriving multiple keys from a single starting point known as a seed. This seed is all that is needed to restore a wallet if it is lost and can allow the creation of public addresses without the knowledge of the private key.

[0265] Difficulty: This number determines how difficult it is to bash a new block. It is related to the maximum allowed number in a given numerical portion of a transaction block's hash. The lower the number, the more, difficult it is to produce a hash value that fits it. Difficulty varies based on the amount of computing power used by miners on the bitcoin network. If large numbers of miners leave a network the difficulty would decrease.

[0266] Digital Certificate: Pieces of code that protect messages without the encrypt-decrypt operations but users must apply (and pay an annual fee) for individual certificates and most common e-mail services do not support them (Google, Outlook, Yahoo).

[0267] Digital Commodity: A digital commodity is a scarce, electronically transferrable, intangible, with a market value.

[0268] Digital Identity: A digital identity is an online or networked identity adopted or claimed in cyberspace by an individual, organization or electronic device.

[0269] Distributed Autonomous Enterprise [DAE]: Requires little or no traditional management or hierarchy to generate customer value and owner wealth.

[0270] Distributed Application [DAPP]: A set of smart contracts that stores data on a home-listings blockchain.

[0271] Distributed Capitalism: Lowering barriers to participation.

[0272] Distributed Ledger: Distributed ledgers are a type of database that are spread across multiple sites, countries or institutions. Records are stored one after the other in a continuous ledger. Distributed ledger data can he either "permissioned" or "unpermissioned" to control who can view it.

[0273] Double Spending: The act of spending bitcoins twice. It happens when someone makes a transaction using bitcoins, and then makes a second purchase from someone else, using the same bitcoins. They then convince the rest of the network to confirm only one of the transactions by hashing it in a block. Double spending is not easy to do, thanks to the way that the bitcoin network operates, but it is nevertheless a risk run by those accepting zero-confirmation transactions.

[0274] Dust: A transaction output that is smaller than a typically fee required to spend it [sic]. This is not a strict part of the protocol, as any amount more than zero is valid. BitcoinQT refuses to mine or relay "dust" transactions to avoid uselessly increasing the size of unspent transaction outputs (UTXO) index.

[0275] Dust Transaction: A transaction for an extremely small amount of bitcoins, which offers little financial value, but takes up space in the blockchain. The bitcoin developer team has taken efforts to eliminate dust transactions by increasing the minimum transaction amount that will be relayed by the network.

E

[0276] ECDSA: The Elliptic Curve Digital Signature Algorithm is the lightweight cryptographic algorithm used to sign transactions in the Bitcoin protocol.

[0277] Elliptic Curve Arithmetic: A set of mathematical operations defined on a group of points on a 2D elliptic curve. Bitcoin protocol uses predefined curve secp256k1. Here is the simplest possible explanation of the operations: you can add and subtract points and multiply them by an integer. Dividing by an integer is computationally infeasible (otherwise cryptographic signatures will not work). The private is a 256-bit integer and the public key is a product of a predefined point G ("generator") by that integer: A-G* a. Associativity law allows implementing interesting cryptographic schemes like Diffie-Hellman key exchange (ECDH): two parties with private keys a and b may exchange their public keys A and B compute a shared secret point C:C+A* b=B* a because(G*a) (G*b)*a. The this point C can be used as a AES encryption key to protect their communication channel.

[0278] 'Entertainment': states, displays, user experience, stimuli (light, sound, tactile), Title/Value Transfer, game

[0279] Escrow: The act of holding funds or assets in a third-party account to protect them during an asynchronous transaction.

[0280] ETF: Acronym for "Exchange Traded Fund". These are investment funds traded on stock markets that track the price index of an underlying asset.

[0281] Ethereum Browser: (aka Ethereum Reference Client) A cross-platform GUI of an interface similar to a simplified browser (a la Chrome) that is able to host sandboxed applications whose backend is purely on the Ethereum protocol.

[0282] Ethereum Runtime Environment: (aka ERE) The environment which is provided to an Autonomous Object executing in the EVM. Includes the EVM but also the structure of the world state on which the EVM relies for certain I/O instructions including CALL & CREATE.

[0283] Ethereum Virtual Machine: (aka EVM) The virtual machine that forms the key part of the execution model for an Account's associated EVM Code.

[0284] EVM Assembly: The human-readable form of EVM code.

[0285] EVM Code: The bytecode that the EVM can natively execute. Used to formally specify the meaning and ramifications of a message to an Account.

[0286] Exchange: A central resource for exchanging different forms of money and other assets. Bitcoin exchanges are typically used to exchange the cryptocurrency for other, typically fiat, currencies.

[0287] External Actor: A person or other entity able to interface to an Ethereum node, but external to the world of Ethereum. It can interact with Ethereum through depositing signed Transactions and inspecting the blockchain and associated state. Has one (or more) intrinsic Accounts.

[0288] Extra Nonce: A number placed in coinbase script and incremented by a miner each time the nonce 32-hit integer overflows. This is not the required way to continue mining when nonce overflows, one can also change the merkle tree of transactions or change a public key used for collecting a block reward.

F

[0289] Faucet: A technique used when first launching an altcoin. A set number of coins are pre-mined, and given away for free, to encourage people to take interest in the coin and begin mining it themselves.

[0290] Fiat Currency: A currency, conjured out of thin air, which only has value because people say it does. Constantly under close scrutiny by regulators due to its known application in money laundering and terrorist activities. Not to be confused with bitcoin.

[0291] Fill or Kill: This is a simple type of buy order made with a cryptocurrency exchange. The investor dictates how much currency they want, and at what price, and establishes a cutoff date for the order. The exchange will then do their best to fill the order according to those criteria. If the exchange hasn't found an appropriate match for the order by the cutoff date, the order is canceled and left unfilled. In other words, fill this order according to these guidelines and within this time frame. If you can't, kill it.

[0292] FinCEN: The Financial Crimes Enforcement Network, an agency within the US Treasury Department. FinCEN has thus far been the main organization to impose regulations on exchanges trading in bitcoin.

[0293] Fork: The creation of an alternative ongoing version of the blockchain, typically because one set of miners begins hashing a different set of transaction blocks from another. It can be caused maliciously, by a group of miners gaining too much control over the network (see 51% attack), accidentally, thanks to a bug in the system, or intentionally, when a core development team decides to introduce substantial new features into a new version of a client. A fork is successful if it becomes the longest version of the blockchain, as defined by difficulty.

[0294] FPGA: A Field Programmable Gate Array is a processing chip that can be configured with custom functions after it has been fabricated. Think of it as a blank silicon slate on which instructions can be written. Because FPGAs can he produced en masse and configured after fabrication, manufacturers benefit from economies of scale, making them cheaper than ASIC chips.

[0295] Freicoin: A cryptocurrency based on the inflation-free principles outlined by the economist Silvio Gessell.

[0296] Frictionless: In reference to payment systems, a system is "frictionless" when there are zero transaction costs or restraints on trading.

[0297] Full Node: A node which implements all of bitcoin protocol and does not require trusting any external service to validate transactions. It is able to download and validate the entire blockchain. All full nodes implement the same peer-to-peer messaging protocol to exchange transactions and blocks, but that is not a requirement. A full node may receive and validate data using any protocol and from any source. However, the highest security is achieved by being able to communicate as fast as possible with as many nodes as possible.

G

[0298] Gas: The fundamental network cost unit. Paid for exclusively by Ether (as of PoC-4), which is converted freely to and from Gas as required. Gas does not exist outside of the internal Ethereum computation engine; its price is set by the Transaction and miners are free to ignore Transactions whose Gas price is too low.

[0299] Genesis Block The very first block in the block chain.

[0300] Gigahashes/sec: The number of hashing attempts possible in a given second, measured in billions of hashes (thousands of Megahashes).

[0301] GPU: Graphical Processing Unit. A silicon chip specifically designed for the complex mathematical calculations needed to render millions of polygons in modern computer game graphics. They are also well suited to the cryptographic calculations needed in cryptocurrency

[0302] Graph Gaps: On occasion, gaps will appear in trend lines on market value graphs. These gaps indicate a visible drop or rise in a commodity's value that hasn't necessarily happened due to trading. These can be the result of closed markets, statistical adjustments by analysts, or by strong news about the commodity. There are three types of gaps:

[0303] 1. Breakaway Gap, These appear at the beginning of a strong upward or downward trend, and represent very high-volume trading.

[0304] 2. Runaway Gap. These occur during an upward or downward trend, and represent a quick momentary intensification of that trend.

[0305] 3. Exhaustion Gap. This occurs toward the end of an upward or downward trend, and tends to indicate a small trend in the opposite direction

H

[0306] Halving: Bitcoins have a finite supply, which makes them a scarce digital commodity. The total amount of bitcoins that will ever be issued is 21 million. The number of bitcoins generated per block is decreased 50% every four years. The final halving will take place in the year 2140.

[0307] Hard Fork: Some people use term hard fork to stress that changing Bitroin protocol requires overwhelming majority to agree with it, or some noticeable part of the economy will continue with original blockchain following the old rules.

[0308] Hardware Wallet: A bitroin wallet which stores users bitcoins offline on hardware devices.

[0309] Hash: A mathematical process that takes a variable amount of data and produces a shorter, fixed-length output. A hashing function has two important characteristics. Firstly, it is mathematically difficult to work out what the original input was by looking at the output. Secondly, changing even the tiniest part of the input will produce an entirely different output.

[0310] to HASH: To compute a hash function of some data. If hash function is not mentioned explicitly, it is the one defined by the context. For instance, "to hash a transaction" means to compute Hash256 of binary representation of a transaction.

[0311] SHA-256 hashed with RIPEMD-160 it is used to produce an address because it makes a smaller hash (20 bytes vs. 32 bytes) than SHA-256, but still uses SHA-256 internally for security, BTCHash160 in CoreBitcoin. Hash160( ) BitcoinQT. It is also available in scripts as OP_HASH160.

[0312] Hash, Hash256: When not speaking about arbitrary hash functions, Hash refers to two rounds of SHA-256. That is, you should compute a SHA-256 hash of your data and then another SHS-256 hash of that hash. It is used in block header hashing, transaction hashing, making a merkle tree of transactions, or computing a checksum of an address.

Known asBTCHash2560( ) in CoreBitcoin, Hash( ) in BitcoinQT. It is also available in scripts as OP_HASH256.

[0313] Hash Function: A hash function takes an arbitrary input such as a string of integers (a key) and outputs a value of a pre-specified length (a hash). Bitcoin uses a cryptographic hash function to secure the network.

[0314] Hash Rate: The number of hashes that can be performed by a bitcoin miner in a given period of time (usually a second).

[0315] Hash Type (hashtype): A single byte appended to a transaction signature in the transaction input which describes how the transaction should be hashed in order to verify that Signature. There are three types affecting outputs: ALL (default), SINGLE, NONE and one optional modifier ANYONECANPAY affecting the inputs (can be combined with either of the first three). ALL requires all outputs to be hashed (thus, all outputs are signed). SINGLE clears all output scripts but the one with the same index as the input in question. NONE clears all outputs thus allowing changing them at will. ANYONECANPAY removes all inputs except the current one (allows anyone to contribute independently.) The actual behavior is more subtle than this overview, you should check the actual source code for more comments.

[0316] Height: See Block Height

[0317] Hot Wallet: A bitcoin wallet that has an active connection to the Internet. These are used, for "everyday" transactions and should never hold large amounts of bitcoin, since their connectivity reduces their security.

[0318] HTML: Acronym for "HyperText Markup Language", the language in which webpages are written.

[0319] HTTP: Acronym for "HyperText Transfer Protocol", this is the underlying protocol for the world wide web.

[0320] Hybrid Wallet: This is a cryptocurrency storage and maintenance system that is a combination of a software wallet (stored on a local computer) and a web wallet (stored on a third-party server). The bulk of your digital currency account information is stored on the wallet host's server—except for one important detail. Your private key (the code that uniquely identifies you) is stored only on your own device. When you make a transaction, your private key is encrypted on the way to the exchange's server, so they never know what your private key is. Access to your private key also includes a password that again only the user knows. If the user loses or forgets that password, access to the account could be denied, and the user could potentially lose the account balance forever.

I

[0321] Industrial Blockchain: Secure transactional capability to watches and other wearable devices.

[0322] Input: The part of a bitcoin transaction denoting where the bitcoin payment has come from. Typically, this will be a bitcoin address, unless the transaction is a generation transaction, meaning that the bitcoin has been freshly mined (see Coinbase).

[0323] Interface System and methods by which two or more computers talk to each other over a network, such as the Internet, using a common language that they both understand.

[0324] Key: Could mean art ECDSA public or private key, or AES symmetric encryption key. AES is not used in the protocol itself (only to encrypt the ECDSA keys and other sensitive data), so usually the word key means an ECDSA key. When talking about keys, people usually mean private keys as public key can always be derived from a private one. See Private Key and Public Key.

[0325] Key Pool: Some wallet applications that create new private keys randomly keep a pool of unused pre-generated keys (BitcoinQT keeps 100 keys by default). When a new key is needed for change address or a new payment request, the application provides the oldest key from the pool and replaces it with a fresh one. The purpose of the pool is to ensure that recently used keys are always already back up on external storage. Without a key pool you could create a new key, receive a payment on its address and then have your hard disk died before backing up this key. A key pool guarantees that this key was already backed up several days before being used. Deterministic wallets do not use a key pool because they need to back up a single secret key.

[0326] Kilohashes/sec: The number of hashing attempts possible in a given second, measured in thousands of hashes.

[0327] Kimuto Gravity Well: A mining difficult readjustment algorithm, which was created in 2013 for Megaroin, an altcoin. The well allows difficulty readjustment to occur every block, instead of every 2016 blocks for Bitcoin. This was done as a response to concern about multi pool mining schemes.

[0328] KYC: Know Your Client/Customer rules force financial institutions to vet the people they are doing business with, ensuring that they are legitimate.

L

[0329] Laundry: Also known as a "mixing service", they combine funds from various users and redistribute them, making tracing the bitcoins back to their original source very difficult by mixing their "taint".

[0330] Ledger: An append-only record store, where records are immutable and may hold more general information than financial records.

[0331] Ledger of Everything: Blockchain can address the six obstacles to a functioning Internet of Things features: resilient, robust, real-time, responsive, radically open, renewable, redactive, revenue-generating, reliable.

[0332] Leverage: In foreign currency trading, leverage multiplies the real funds in your account by a given factor, enabling you to make trades that result in significant profit. By giving leverage to a trader, the trading exchange is effectively lending them money, in the hope that it will earn back more than it loaned in commission. Leverage is also known as a margin requirement.

[0333] Lightweight Client: Comparing to full node, lightweight node does not store the whole blockchain and thus cannot fully verify any transaction. There are two kinds of lightweight nodes: those fully trusting an external service to determine wallet balance and validity of transactions (e.g., Blockchain.info) and the apps implementing Simplified Payment Verification (SPV). SPV clients do not need to trust any particular service, but are more vulnerable to 51% attack than full nodes. See Simplified Payment Verification.

[0334] Litecoin: An altcoin based on the Scrypt proof of work.

[0335] Liquidity: The ability to buy and sell an asset easily, with pricing that stays roughly similar between trades. A suitably large community of buyers and sellers is important for liquidity. The result of an illiquid market is price volatility, and the inability to easily determine the value of an asset.

[0336] Liquidity Swap: As a financial instrument on cryptocurrency exchanges, liquidity swaps are contracts where investors offer loans to others to trade with in exchange for a set return.

[0337] LLL: The Lisp-like Low-level Language, a human-writable language used for authoring simple contracts and general low-level language toolkit for trans-compiling to.

[0338] Lock Time (locktime): A 32-bit field in a transaction that means either a block height at which the transaction becomes valid, or a UNIX timestamp. Zero means transaction is valid in any block. A number less than 500000000 is interpreted as a block number (the limit will he hit after year 11000), otherwise a timestamp.

[0339] Lottery: Defined by many states as prize, chance & consideration.

M

[0340] MAC Media Access Control.

[0341] Main Chain: A part of the blockchain which a node considers the most difficult (see difficulty). All nodes store all valid blocks, including orphans and recompute the total difficulty when receiving another block. If the newly arrived block or blocks do not extend existing main chain, but create another one from some previous block, it is called reorganization.

[0342] Mainnet: Main Bitcoin network and its blockchain. The term is mostly used in comparison to testnet.

[0343] mBTC: 1 thousandth of a bitcoin (0.001 BTC).

[0344] Megahashes/sec: The number of hashing attempts possible in a given second, measured in millions of hashes (thousands of kilohashes).

[0345] Mempool: A technical term for a collection of unconfirmed transactions stored by a node until they either expire or get included in the main chain. When reorganization happens, transactions from orphaned blocks either become invalid (if already included in the main chain) or moved to a pool of unconfirmed transactions. By default, bitcoind nodes throw away unconfirmed transactions after 24 hours.

[0346] Merged Mining: This allows a miner to work on multiple blockchains simultaneously, contributing to the hash rate (and thus security) of both currencies being mined. E.g. Namecoin has implemented merged mining with Bitcoin.

[0347] Merkle Tree: Merkle tree is an abstract data structure that organizes a list of data items in a tree of their hashes (like in Git, Mercurial or ZFS). In Bitcoin the merkle tree issued only to organize transactions within a block (the block header contains only one hash of a tree) so that full nodes may prune fully spent transactions to save disk space, SPV clients store only block headers and validate transactions if they are provided with a list of all intermediate hashes.

[0348] Message: Data (as a set of bytes) and Value (specified as Ether) that is passed between two Accounts, either through the deterministic operation of an Autonomous Object or the cryptographically secure signature of the Transaction.

[0349] Message Call: The act of passing a message from one Account to another. If the destination account is associated with non-empty EVM Code, then the VM will be started with the state of said Object and the Message acted upon. If the message sender is an Autonomous Object, then the Call passes any data returned from the VM operation.

[0350] Microtransaction: Paying a tiny amount for an asset or service, primarily online. Micro-transactions are difficult to perform under conventional payment systems, because of the heavy commissions involved. It is difficult to pay two cents to read an online article using your credit card, for example.

[0351] Miner: A computer participating in any cryptocurrency network performing proof of work. This is usually done to receive block awards.

[0352] Mining: The act of generating new bitcoins by solving cryptographic problems using computing hardware.

[0353] Mining Algorithm: The algorithm used by a cryptocurrency to sign transactions in the Bitcoin network, adding blocks onto the blockchain.

[0354] Mining Contract: A method of investing in bitcoin mining hardware, allowing anyone to rent out a pre-specified amount of hashing power, for an agreed amount of time. The mining service takes care of hardware maintenance, hosting and electricity costs, making it simpler for investors.

[0355] Mining Pool: A group of miners who have decided to combine their computing power for mining. This allows rewards to be distributed more consistently between participants in the pool.

[0356] Mint: Satoshi distributed the mint by linking the issuance of bitcoins to the creation of a new block ledger, putting the power to mint into all the hands of the peer network.

[0357] Mintage Cap: As cryptocurrency miners process blocks of transaction data, they generate new coins as a result. Cryptocurrency is a young industry, and its issuers want enough coins to go around to satisfy new investors as they join. These new coins are mathematically designed to be turned out at a stable rate, so the value of the currency will remain relatively stable, too (there will be fluctuations, as in any other commodity market, but not as wild as they would be if the commodity was extremely limited in availability). Over time, however, the mathematics of coin creation are also designed to end, to avoid over-saturation of the market and currency devaluation.

[0358] Minting: the process of rewarding users in proof of stake coins. New coins are minted as the reward for verifying transactions in a block.

[0359] Mixing: A process of exchanging coins with other persons in order to increase privacy of one's history. Sometimes it is associated with money laundering, but strictly speaking it is orthogonal to laundering. In traditional banking, a bank protects customer's privacy by hiding transactions from all 3^{rd} parties. In Bitcoin any merchant may do a statistical analysis of one's entire payment history and determine, for instance, how many bitcoins one owns. While it is still possible to implement KYC (Know Your Customer) rules on a level of every merchant, mixing allows to be separate information about one's history between the merchants. Most important use cases for mixing are: 1) receiving a salary as a single bit monthly payment and then spending it in small transactions ("café sees thousands of dollars when you pay just $4"); 2) making a single payment and revealing connection of many small private spendings ("car dealer sees how much you are addicted to the coffee"), in both cases your employer, a cafe and a car dealer may comply with KYC/AML laws and report your identity and transferred amounts, but neither of them need to know about each other. Mixing bitcoins after receiving a salary and mixing them before making a big payment solves this privacy problem.

[0360] Mixing Service: Service that mixes your bitcoins with someone else's, sending you back bitcoins with different inputs and outputs from the ones that you sent to it. A mixing service (also known as a tumbler) preserves your privacy because it stops people tracing, a particular bitcoin to you. It also has the potential to be used for money laundering.

[0361] Mobile Wallet: A wallet which runs a "Mobile client", allowing people to have bitcoin wallets on their phones and tablet computers and pay on the go.

[0362] Monetary Policy: Another breakthrough is to preserve value programmed into the software.

[0363] Money Laundering: The act of trying to "clean" money earned from criminal activity by converting these profits to what appear to be legitimate assets.

[0364] M-of-N Multi-signature Transaction: A transaction that can be spent using M signatures when N public keys are required (M is less or equal to N). Multi-signature transactions that only contain one OP_CHECKMULSIG opcode and N is 3, 2 or 1 are considered standard.

[0365] Multisig: Multi-signature addresses allow multiple parties to partially seed an address with a public key. When someone wants to spend some of the bitcoins, they need some of these people to sign their transaction in addition to themselves. The needed number of signatures is agreed at the start when people create the address. Services using multi-signature addresses have a much greater resistance to theft.

N

[0366] Namecoin: An altcoin designed to provide an alternative to the traditional domain name system (DNS). Users can register .bit domains, accessible via proxy servers, by paying with namecoins.

[0367] Network Effect: The increase in value of a good or service that occurs when its use becomes more widespread.

[0368] NFC: Acronym for "Near Field Communication", a low power, short range method of wireless communication. This can be used to build upon RFID systems and is what contactless smart cards (oyster cards) and payment systems (paypass) use. Most recently implement in the Apple Pay app.

[0369] Node: A computer connected to the bitcoin network using a client that relays transactions to others (see client).

[0370] Nonce: A random string of data used as an input when hashing a transaction block. A nonce is used to try and produce a digest that fits the numerical parameters set by the bitcoin difficulty. A different nonce will be used with each hashing attempt, meaning that billions of nonces are generated when attempting to hash each transaction block.

[0371] Non-standard Transaction: Any valid transaction that is not standard. Non-standard transactions are not relayed or mined by default BitcoinQT nodes (but are relayed and mined on testnet). However, if anyone puts such transaction in a block, it will be accepted by all nodes. In practice it means that unusual transactions will take more time to get included in the blockchain. If some kind of non-standard transactions becomes useful and popular, it may get named standard and adopted by users (like it). See Standard Transaction.

[0372] Novacoin: Though this type of cryptocurrency is not yet near the value or overall investor numbers of the big players in the industry. Novacoin still holds a spot in the top five; not bad, considering it was introduced in February 2013. Novacoin used the Scrypt mining algorithm, and is mined by the combined proof-of-work and proof-of-stake methods.

O

[0373] Object: Synonym for Autonomous Object.

[0374] Off Blockchain Transactions: Exchanges of value which occur off the blockchain between trusted parties. These occur because they are quicker and do not block the blockchain.

[0375] Off-Ledger Currency: A currency minted off-ledger and used on-ledges. An example of this would be using distributed ledgers to manage a national currency.

[0376] On-Ledger Currency: A currency minted on-ledger and used on-ledger. An example of this would be cryptocurrency.

[0377] Opcode: 8-bit code of script operation. Codes from 0x01 to 0x4B (decimal 75) are interpreted as a length of data to be pushed on the stack of the interpreter (data bytes follow the opcode). Other codes are either do some interesting, or disabled and cause transaction verification to fail, or do nothing (reserved for future use).

[0378] Open Network Enterprises: As smart contracts grow in complexity and interoperate with other contracts then contribute to this.

[0379] Open Source: The practice of sharing the source code for a piece of computer software, allowing it to be distributed and altered by anyone.

[0380] Orphan Block: A block which is not a part of the valid blockchain, but which was instead pin of a fork that was discarded.

[0381] OTC Exchange: An exchange in which traders make deals with each other directly, rather than relying on a central exchange to mediate between them.

[0382] Output: The destination address for a bitcoin transaction. There can he multiple outputs for a single transaction.

[0383] Owners of Coin: Ethereum chose this as its economic set. Ripple and Stellar chose the social network.

[0384] Owners of the Computing Power: Satoshi chose this economic set. This requires these miners to consume a resource external to the network, namely electricity, if they want to participate in the reward system.

[0385] Paper Wallet: A printed sheet containing one or more public bitcoin addresses and their corresponding private keys. Often used to store bitcoins securely, instead of using software wallets, which can be corrupted, or web wallets, which can be hacked or simply disappear. A useful form of cold bitcoin storage.

[0386] Participant: An actor who can access the ledger: read records or add records to,

[0387] Pay-to-Script Hash: A type of script and address that allows sending bitcoins to arbitrary complex scripts using a compact hash of that script. This allows payer to pay, much smaller transaction fees and not wait very long for a non-standard transaction to get included in the blockchain. Then the actual script matching the hash must be provided by the payee when redeeming the funds. P2SH addresses are encoded in Base58 Check just like regular public keys and start with number "3".

[0388] Peer: An actor that shares responsibility for maintaining the identity and integrity of the ledger.

[0389] P2P: Peer-to-peer. Decentralized interactions that happen between at least two parties in a highly interconnected network. An alternative system to a 'hub-and-spoke' arrangement, in which all participants in a transaction deal with each other through a single mediation point.

[0390] Permissioned Ledger: A permissioned ledger is a ledger where actors must have permission to access the ledger. Permissioned ledgers may have one or many owners. When a new record is added, the ledger's integrity is checked by a limited consensus process. This is carried out by trusted actors—government departments or banks, for example—which makes maintaining a shared record much simpler that the consensus process used by unpermissioned ledgers. Permissioned block chains provide high-verifiable data sets because the consensus process creates a digital signature, which can be seen by all parties. A permissioned ledger is usually faster than an unpermissioned ledger.

[0391] Phone-to-Phone Transfer: This is a mobile application feature that allows the instantaneous transfer of information from one smartphone to another if two mobile device users want to exchange data, and both have this feature installed and activated on their phones, they can make the transfer simply by having their devices in dose proximity to each other. These are also sometimes called "touch transfers."

[0392] Platform Exchange: This is a digital currency exchange that limits the role they play in transactions made between investors. The majority of exchanges are there to facilitate these transactions, and make them easier to carry out. The exchange will son through buy and sell orders, and will then match no investors who meet the criteria of the order in question. Their algorithms are designed so the trades being made are both secure and fair to both parties involved. Beyond that, however, the exchange does not play any "middleman" or mediating role. This is in contrast to exchanges that will hold the transaction funds in escrow, or will discuss the details of the trade with both investors before moving forward.

[0393] Pool: A collection of mining clients which collectively mine a block, and then split the reward between them. Mining pools are a useful way to increase your probability of successfully mining a block as the difficulty rises.

[0394] PPCoin: AKA Peercoin or P2P coin. An altcoin using the proof of stake mechanism conjunction with proof of work. Based on a paper produced by Sunny King and Scott Nadal.

[0395] Pre-mining: The mining of coins by a cryptocurreney's founder before that coin has been announced and details released to others who may wish to mine the coin. Pre-mining is a common technique used with scamcoins, although not all pre-mined coins are scamcoins (see Scamcoin).

[0396] Primecoin: Developed by Sunny King, Primecoin uses a proof of work system to calculate prime numbers.

[0397] Private Key (PrivKey): An alphanumeric string kept secret by the user, and designed to sign a digital communication when hashed with a public key. In the case of bitcoin, this string is a private key designed to work with a public key. The public key is a bitcoin address (see Bitcoin Address).

[0398] Process Node: The size of a transistor in nanometers, produced during a chip fabrication process. Smaller process nodes are more efficient.

[0399] Proof of Activity: Combines proof of work and proof of stake.

[0400] Proof of Burn: This is a method of "burning" one Proof of Work cryptocurrency in order to receive a different cryptocurrency. This is a form of "bootstrapping" one cryptocurrency off another, and is done by sending coins to a verifiable unspendable address.

[0401] Proof of Capacity: Requires miners to allot a sizeable volume of their hard drive to mining.

[0402] Proof of Existence: A service provided through the blockchain that allows anyone to anonymously and securely store a proof of existence for any document they choose online. This allows people to prove that a document existed at a certain point in time and demonstrate their ownership of it, without fear of that proof being taken from them.

[0403] Proof of Stake: An alternative to proof of work, in which your existing stake in a currency (the amount of that currency that you hold) is used to calculate the amount of that currency that you can mine.

[0404] Proof of Storage: Requires miners to allocate and share disk space in distributed cloud.

[0405] Proof of Work: A system that ties mining capability to computational power. Blocks must he hashed, which is in itself an easy computational process, but an additional variable is added to the hashing process to make it more difficult. When a block is successfully hashed, the hashing must have taken some time and computational effort. Thus, a hashed block is considered proof of work.

[0406] Prosumers: Customers who produce.

[0407] Protocol Evolution: Blockchain is the result of the natural evolution of internet protocols. Wired explains the story of how the original 1974 TCP/IP Internet network protocol and Tim Berner-Lee's Hyper Text Transfer Protocol (HTTP) evolved in the same way as blockchain is evolving for the next generation of the Internet, bundling multiple protocols together to form the foundation of future frameworks and "watching the birth of the internet over again".

[0408] PSP: Payment Service Provider. The PSP offers payment processing services for merchants who wish to accept payments online.

[0409] P2SH: See Pay-to-Script Has.

[0410] Public Key (Pubkey); An alphanumeric string which is publicly known, and which is hashed with another, privately held string to sign a digital communication. In the case of bitcoin, the public key is a bitcoin address.

Q

[0411] QR Code: A two-dimensional graphical block containing a monochromatic pattern representing a sequence of data, QR or "Quick Response" codes are designed to be scanned by cameras, including those found in mobile phones, and are frequently used to encode bitcoin addresses.

R

[0412] Reference Implementation: Bitcoin QT (or bitcoind) is, the most used full node implementation, so it is considered a reference for other implementations. If an alternative implementation is not compatible with BitcoinQT it may be forked, that is it will not see the same main chain as the rest of the network running BitcoinQT.

[0413] Relaying Transactions: Connected Bitcoin nodes relay new transactions between each other on best effort basis in order to send them to the mining nodes. Some transactions may not be relayed by all nodes. E.g., non-standard transactions, or transactions without a minimum fee. Bitcoin message protocol is not the only way to send the transaction. One may also send it directly to a miner, mine it yourself, or send it directly to the payee and make them to relay or mine it.

[0414] Remittance: A sum of money being sent, usually internationally, as a payment or gift.

[0415] Reorg, Reorganization: An event in the node when one or more blocks in the main chain become orphaned. Usually, newly received blocks are extending existing main chain. Sometimes (4.6 times a week) a couple of blocks of the same height are produced almost simultaneously and for a short period of time some nodes may see one block as a tip of the main chain which will be eventually replaced by a more difficult blocks(s). Each transaction in the orphaned blocks either becomes invalid (if already included in the main chain block) or becomes unconfirmed and moved to the mempool. In case of a major bug or a 51% attack, reorganization may involve reorganizing more than one block.

[0416] Replicated Ledger: A ledger with one master (authoritative) copy of the data, and many slave (non-authoritative) copies.

[0417] Reward: Amount of newly generated bitcoins that a miner may claim in a new block. The first transaction in the block allows miner to claim currently allowed reward as well as transaction fees from all transactions fees from all transactions in the block. Reward is halved ever 210000 blocks approximately every 4 years. As of Jul. 27, 2014 the reward is 25 BTC (the first halving occurred in December 2012). For security reasons, rewards cannot be spent before 100 blocks built on top of the current book.

[0418] Ripple: A payment network that can be used to transfer any currency (including ad hoc currencies that have been created by users). The network consists of payment nodes and gateways operated by authorities. Payments are made using a series of IOUs, and the network is based on trust relationships,

S

[0419] Satoshi: The smallest subdivision of a bitcoin currently available (0.00000001 BTC).

[0420] Satoshi Nakamoto: The name used by the original inventor of the Bitcoin protocol, who withdrew from the project at the end of 2010.

[0421] Scamcoin: An altcoin produced with the sole purpose of making money for the originator. Scamcoins frequently use pump and dump techniques and pre-mining together.

[0422] Script: A compact turing-incomplete programming language used in transaction inputs and outputs. Scripts are interpreted by a Forth-like stack machine: each operation manipulates data on the stack. Most scripts follow the standard pattern and verify the digital signature provided in the transaction input against a public key provided in the previous transaction's output. Both signatures and public keys are provided using scripts. Scripts may contain complex conditions, but can never change amounts being transferred. Amount is stored in a separate field in a transaction output.

[0423] scriptPubKey: Original name in bitcoind for a transaction output script. Typically, output scripts contain public keys (or their bashes: see Address) that allow only owner of a corresponding private key to redeem the bitcoins in the output.

[0424] scriptSig: Original name in bitcoind for a transaction input script. Typically, input scripts contain signatures to prove ownership of bitcoins sent by a previous transaction.

[0425] Scrypt: An alternative proof of work system to SHA-256, designed to be particularly friendly to CPU and GPU miners, while offering little advantage to ASIC miners.

[0426] Secret Key: Either the Private Key or an encryption key is used in encrypted wallets. Bitcoin protocol does not use encryption anywhere, so secret key typically means a private key used for signing transactions.

[0427] Sequence: A 32-bit unsigned integer in a transaction input used to replace older version of a transaction by a newer one. Only used when locktime is not zero. Transaction is not considered valid until the sequence number is 0xFFFFFFFF.

[0428] Seed: The private key used in a "deterministic wallet".

[0429] Self-Executing Contract: Also known as "smart contracts" these are protocols that facilitate or enforce the obligations of contract without the need for human intervention.

[0430] SEPA: The Single European Payments Area. A payment integration agreement within the European Union, designed to make it easier to transfer funds between different banks and nations in euros.

[0431] SHA-256: The cryptographic function used as the basis for bitcoin's proof of work system.

[0432] Sidechain: These are theoretical, independent blockchains which are "two way pegged" to the Bitcoin blockchain. These can have their own unique features and can have bitcoins sent to and from them.

[0433] Signature: A digital digest produced by hashing private and public keys together to prove that a bitcoin transaction came from a particular address.

[0434] Simplified Payment Verification (SPV): A scheme to validate transactions without storing the whole blockchain (only block headers) and without trusting any external service. Every transaction must be present with all its parent and sibling hashes in a merle tree up to the root. SPV client trusts the most difficult chain of block headers and can validate if the transaction indeed belongs to a certain block header. Since SPV does not validate all transactions, a 51% attack may not only cause a double spend (like with full nodes), but also make a completely invalid payment with bitcoins created from nowhere. However, this kind of attack is very costly and probably more expensive than a product in question. Bitcoinj library implements SPV functionally. (See SPV)

[0435] Smart Contracts: Smart contracts are contracts whose terms are recorded in a computer language instead of a legal language. Smart contracts can be automatically executed by a computing system, such as a suitable distributed ledger system.

[0436] Soft Fork: Sometimes the soft fork refers to an important change of software behavior that is not a hard fork (e.g., changing mining fee policy). See Hard Fork and Fork.

[0437] Source Code: The open-source software which includes protocols governing rules for movement and ownership of bitcoins and the cryptography system that secures and verifies Bitcoin transactions.

[0438] Speculator: An individual who speculates on the price of bitcoin or any other form asset. Aiming to make profits by buying and selling at different prices.

[0439] Spent Output: A transaction output can be spent only once: when another valid transaction makes a reference to this output from its own input. When another transaction attempts to spend the same output, it will be rejected by the nodes already seeing the first transaction. Blockchain as a proof-of-work scheme allows every node to agree on which transaction was indeed the first one. The whole transaction is considered spent when all its outputs are spent.

[0440] Split: A split of a blockchain. See Fork.

[0441] SPY: Simplified Payment Verification. A feature of the Bitcoin protocol that enables nodes to verify payments without downloading the full blockchain. Instead, they need only download block headers.

[0442] Stale: When a bitcoin block is successfully hashed, any others attempting to hash it may as well stop, because it is now 'stale'. They would simply be repeating work that someone else has already done, for no reward. The term is also used in mining pools to describe a share of a bashing job that has already been completed.

[0443] Stale Block: A block that has already been solved and thus cannot offer miners any reward for further work on it.

[0444] Standard Transaction: Some transactions are considered standard, meaning they are relayed and mined by most nodes. More complex transactions could be buggy or cause DoS attacks on the network, so they are considered non-standard and not relayed or mined by most nodes. Both standard and non-standard transactions are valid and once included in the blockchain, will be recognized by all nodes. Standard transactions are: 1) sending to a public key, 2) sending to an address, 3) sending to a P2SH address, 4) sending to a M-of-N multi-signature transaction where N is 3 or less.

[0445] Storage State: The information particular to a given Account that is maintained between the times that the Account's associated EVM Code runs.

T

[0446] Taint: An analysis of how closely related two addresses are when they have both held a particular bitcoin. A taint analysis could be used to determine how many steps it took for bitcoins to move from an address known for stolen coins, to the current address.

[0447] Target: A 256-bit number that puts an upper limit for a block header hash to be valid. The lower the target is, the higher the difficult to find a valid has. The maximum (easiest) target is 0x00000000FFFF0000000000000000000000000000 0000000000000000000000. The difficulty and the target are adjusted every 2016 blocks (approx. 2 weeks) to keep interval between the blocks close to 10 minutes.

[0448] TCP/IP: Acronyms stand for "Transmission Control Protocol"/"Internet Protocol" and is the connection protocol used by the Internet.

[0449] Terahashes/sec: The number of bashing attempts possible in a given second, measured in trillions of bashes (thousands of Gigahashes).

[0450] Testnet: An alternative bitcoin blockchain, used purely for testing purposes,

[0451] Testnet3: The latest version of testnet with another genesis block.

[0452] Timestamp: A proof that a piece of data existed at a certain point in time. For Bitcoin this is the cryptographic proof of when transactions have taken place.

[0453] Tokenless Ledger: A tokenless ledger refers to a distributed ledger that doesn't require a native currency to operate.

[0454] TOR: An anonymous routing protocol, used by people wanting to hide their identity online.

[0455] Total Coin Supply: For many cryptocurrencies, there is a limit on the total number of coins that will ever come into existence, bitcoin's total supply is capped at 21 million coins.

[0456] Transaction: A piece of data, signed by an External Actor. It represents either a Message or a new Autonomous Object. Transactions are recorded into each block of the blockchain.

[0457] Transaction Block: A collection of transactions on the bitcoin network, gathered into a block that can then be hashed and added to the blockchain.

[0458] Transaction Database: From a purely technological perspective, blockchains are transaction databases. The hashes, keys and nodes all make up a distributed database that eschews centralized storage.

[0459] Transaction Fee: A small fee imposed on some transactions sent across the bitcoin network. The transaction fee is awarded to the miner that successfully hashes the block containing the relevant transaction.

[0460] Transaction input: A part of a transaction that contains a reference to a previous transaction's output and a script that can prove ownership of that output. The script usually contains a signature and thus called scriptSig. Inputs spend previous outputs completely. So if one needs to pay only a portion of some, previous output, the transaction should include extra change output that sends the remaining portion back to its owner (on the same or different address). Coinbase transactions contain only one input with a zeroed reference to a previous transaction and an arbitrary data in place of script.

[0461] Transaction Output: An output contains an amount to be sent and a script that allows further spending. The script typically contains a public key (or an address, a hash of a public key) and a signature verification opcode. Only an owner of a corresponding private key is able to create another transaction that sends that amount further to someone else, in every, transaction, the sum of output amounts must be equal or less than a sum of all input amounts. See Change.

[0462] TX: see Transaction.

[0463] Txin: Transaction Input.

[0464] Txout: see Transaction Output.

[0465] Ubiquity: Blockchains are everywhere; at this point in the alphabet that is not news. The open source code, universally applicable architecture of blockchains, and their ability to distribute, anonymize, protect, and keep a perfectly accurate record of web transactions makes the technology a given.

[0466] Ubte: One microbitcoin (0.000001 BTC).

[0467] Unconfirmed Transaction: Transaction that is not included in any block. Also known as "0-confirmation." transaction. Unconfirmed transactions are relayed by the nodes and stay in the mempools. Unconfirmed transaction stays the pool until the node decides to throw it away, finds it in the blockchain, or includes it in the blockchain, or includes it in the blockchain itself (if it is a miner). See, Confirmation Number.

[0468] Unique Node List: Other blockchains such as Ripple and Stellar rely on social networks for consensus and may recommend new participants (i.e., new nodes) to generate unique mode list.

[0469] Unpermissioned Ledgers: Unpermissioned ledgers such as Bitcoin have no single owner—indeed, they cannot be owned. The purpose of an unpermissioned ledger is to allow anyone to contribute data to the ledger and for everyone in possession of the ledger to have identical copies. This creates resistance which means that no actor can prevent a transaction from being added to the ledger. Participants maintain the integrity of the ledger by reaching a consensus about its state.

[0470] UTXO Set; A collection of Unspent Transaction Outputs. Typically used in discussions on optimizing an ever-growing index of transaction outputs that are not yet spent. The index is important to efficiently validate newly created transactions. Even if the rate of the new transactions remains constant, the time required to locate and verify unspent output grows. Possible technical solutions include more efficient indexing algorithms and a more performant hardware. BitcoinQT, for example, keeps only an index of outputs matching user's keys and scans the entire blockchain when validating other transactions. A developer of one web wallet service mentioned that they maintain the entire index of UTXO and its size was around 100 Gb when the blockchain itself was only Gb. Some people seek social methods to solve the problem. For instance, by refusing to relay or mine transactions that are considered dust (containing outputs smaller than a transaction fee required to mine/relay them).

[0471] Vanity Address: A bitcoin address with a desirable pattern, such as a name.

[0472] Varint: This term may cause confusion as it means different formats in different Bitcoin implementations. See CompactSize.

[0473] Velocity of Money: The velocity of money is an indicator of how quickly money received is then spent again. For bitcoin, we use "bitcoin days destroyed" to measure its velocity, this can indicate whether people are hoarding or spending their bitcoins.

[0474] Verification: Blockchains would not work as ledgers without verification. Much of this falls on miners, whose block creation software verifies hashes of transactions when bundling them into blocks. In cryptocurrency and banking scenarios, payment verification is also paramount. This verification happens through node communication in the distributed network, cross-checking a Bitcoin transaction against each node's blockchain data before sending it through.

[0475] Virgin Bitcoin: Bitcoins purchased as a reward for mining a block. These have not yet been sent anywhere.

[0476] Volatility: The measurement of price movements over time for a traded financial asset (including bitcoin),

W

[0477] Wallet: A method of storing bitcoins for later use. A wallet holds the private keys associated with bitcoin addresses. The blockchain is the record of the bitcoin amounts associated with those addresses.

[0478] Wallet: Just like a bill-and-coin wallet, this is a place to keep your digital currency. There are four types of cryptocurrency wallets:

[0479] 1. Software Wallet. These are programs you load onto your desktop or laptop computer.

[0480] 2. Mobile Wallet: These come in the form of applications you install on your smartphone or tablet computer. They usually include OR code scanning and phone-to-phone transfers for on-the-go transactions.

[0481] 3. Web Wallet: These are usually gotten through exchanges, and stored on third-party servers via cloud computing. They can be accessed by any computing device.

[0482] 4. Paper Wallet: Your digital currency can be printed out, usually in the form of OR codes, and these hard-copy cryptocurrency "bills" can be kept in a physical wallet just like traditional money.

[0483] Wire Transfer: Electronically transferring money from one person to another. Commonly used to send and retrieve fiat currency from bitcoin exchanges.

X

[0484] XBT: informal currency code for 1 Bitcoin (defined as 100 000 000 Satoshis). Some people proposed using it for 0.01 Bitcoin to avoid confusion with BTC. There were rumors that Bloomberg tests XBT as a ticker for 1 Bitcoin, but currently there is only ticker XBTFUND for SecondMarket's Bitcoin investment Trust. See BTC.

[0485] XRP: Also known as Ripple, XRP is a global payments network built on blockchain that is marketed at international banks. XRP itself is the native currency organizations can use to represent flat currency, cryptocurrency, commodities, or any other unit of value. Ripple is one of the oldest examples of open payment protocols using blockchain, but there is a laundry list of companies with different APIs, platforms and distributed payments networks. Deloitte's Banking Industry Outlook recently released a report estimating that blockchain-based payment systems could equal the volume of the United States Automated Clearing House (ACH) financial transactions network by 2020.

Z

[0486] Zerocoin: A protocol designed, to make cryptocurrency transactions truly anonymous.

[0487] Zero-confirmation Transaction: A transaction in which the merchant is happy to provide a product or service before the bitcoin's transmission has been confirmed by a miner and added to the blockchain. It can carry a risk of double spending.

[0488] Zero-confirmation Transaction: The processing of data for cryptocurrency transactions can take anywhere from half a minute upward to over ten minutes in some cases. Though this is necessary in order to validate transactions, and guards against fraudulent activity such as double spending, the waiting period can be inconvenient for those involved in the transactions. As a result, some exchanges and businesses that deal with digital currency are offering "zero confirmation" transactions, which are almost immediately verified without waiting for the mining process to confirm the data block. Double spending, the practice in which a coin holder applies the same currency to two different transactions is, a concern with zero confirmation transactions. Since cryptocurrency is not "attached" to the person spending it in any way, by the time their double spending is discovered through the mining process, they are long gone and untraceable. With the demand for zero confirmation transactions on the upswing, entrepreneurs in the cryptocurrency industry are looking at ways to instantly verify, or deny, transactions without having to wait for mining to take place. In the meantime, many businesses levy fees to offset the financial risk of zero confirmation transactions, and yet others are refusing to accept them until the technology catches up.)

[0489] Z System: IBM is openly committed to advancing blockchain technology on, many fronts, but the company has even gone as far as offering a Blockchain-as-a-Service (BaaS) platform for developers on the. IBM Cloud, and integrating blockchain-based apps (created through the Hyperledger Project) on IBM a Systems. IBM even plans to leverage blockchains combined with Watson on the Watson IoT platform to make it possible for information from devices such as RFID-based locations, barcode-scan event, or device-reported data to be used with IBM's Blockchain and sync with distributed ledgers and smart contracts.

We claim:

1. A system for control of an entertainment state system, comprising:

an application plane layer, the application layer adapted to receive instructions regarding operation of the entertainment state system, the application plane layer coupled to an application plane layer interface,

a control plane layer, the control plane layer including an adaptive control unit, the control plane layer interfacing with the application plane layer interface to receive information related to the instructions regarding operation of the entertainment state system, the control plane coupled to a control plane layer interface, and

a data plane layer, the data plane layer including an input interface to receive data input from one or more data sources, the data plane layer being coupled to the control plane layer interface.

2. The system for the control of an entertainment state system of claim **1** wherein the adaptive control unit includes cognitive computing unit.

3. The system for control of an entertainment state system of claim **1** wherein the control plane layer includes an artificial intelligence unit.

4. The system for control of an entertainment state system of claim **1** wherein the control plane layer includes a machine-learning unit.

5. The system for control of an entertainment state system of claim **5** wherein the control plane layer includes a neural network.

6. The system for control of an entertainment state system of claim **5** wherein the neural network is a deep neural network.

7. The system for control of an entertainment state system of claim **5** wherein the neural network includes a graphics processing unit (GPU).

8. The system for control of an entertainment state system of claim **5** wherein the neural network is trained utilizing user response data.

9. The system for control of an entertainment state system of claim **5** wherein the neural network is a vectorized neural network.

10. The system for control of an entertainment state system of claim **5** wherein the neural network is a recurrent neural network.

11. The system for control of an entertainment state system of claim **1** wherein the control plan layer further includes an analytics unit.

12. The system for control of an entertainment state system of claim **1**, wherein the control plane layer further includes a processor.

13. The system for control of an entertainment state system of claim **1** wherein the application plane layer includes a graphical user interface unit.

14. The system for control of an entertainment state system of claim **1** wherein the application play layer further includes a processor.

15. The system for control of an entertainment state system of claim **1** wherein the data plane layer includes an input port.

16. The system for control of an entertainment state system of claim **1** wherein the input port is coupled to receive external data.

17. The system for control of an entertainment state system of claim **16** wherein the external data in Internet of Things (IoT) data.

18. The system for control of an entertainment state system of claim **16** wherein the input port is coupled to a processor.

19. The system for control of an entertainment state system of claim **1** wherein the data plane layer includes a graphical user interface (GUI) generator.

20. The system for control of an entertainment state system of claim **19** wherein the graphical user interface is coupled to an output port.

21. The system for control of an entertainment state system of claim **20** wherein the data plane layer includes an output port adapted to couple to a display device.

22. The system for control of an entertainment state system of claim **1** wherein the data plane layer further includes a value transfer element.

23. The system for control of an entertainment state system of claim **1** wherein the data plane layer further includes a title transfer element.

24. The system for control of an entertainment state system of claim **1** wherein the data plane layer further includes a management network element.

25. The system for control of an entertainment state system of claim **1** wherein the data plane layer further includes a control network element.

* * * * *

US 20180373983A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2018/0373983 A1**

Katz et al. (43) **Pub. Date: Dec. 27, 2018**

(54) **ARCHITECTURES, SYSTEMS AND METHODS FOR PROGRAM DEFINED TRANSACTION SYSTEM AND DECENTRALIZED CRYPTOCURRENCY SYSTEM**

(71) Applicant: **MILESTONE ENTERTAINMENT LLC**, Beverly Hills, CA (US)

(72) Inventors: **Randall M. Katz**, Beverly Hills, CA (US); **Robert Tercek**, Hollywood, CA (US)

(21) Appl. No.: **16/052,409**

(22) Filed: **Aug. 1, 2018**

Related U.S. Application Data

(63) Continuation of application No. 15/886,432, filed on Feb. 1, 2018.

(60) Provisional application No. 62/454,423, filed on Feb. 3, 2017.

Publication Classification

(51) **Int. Cl.**

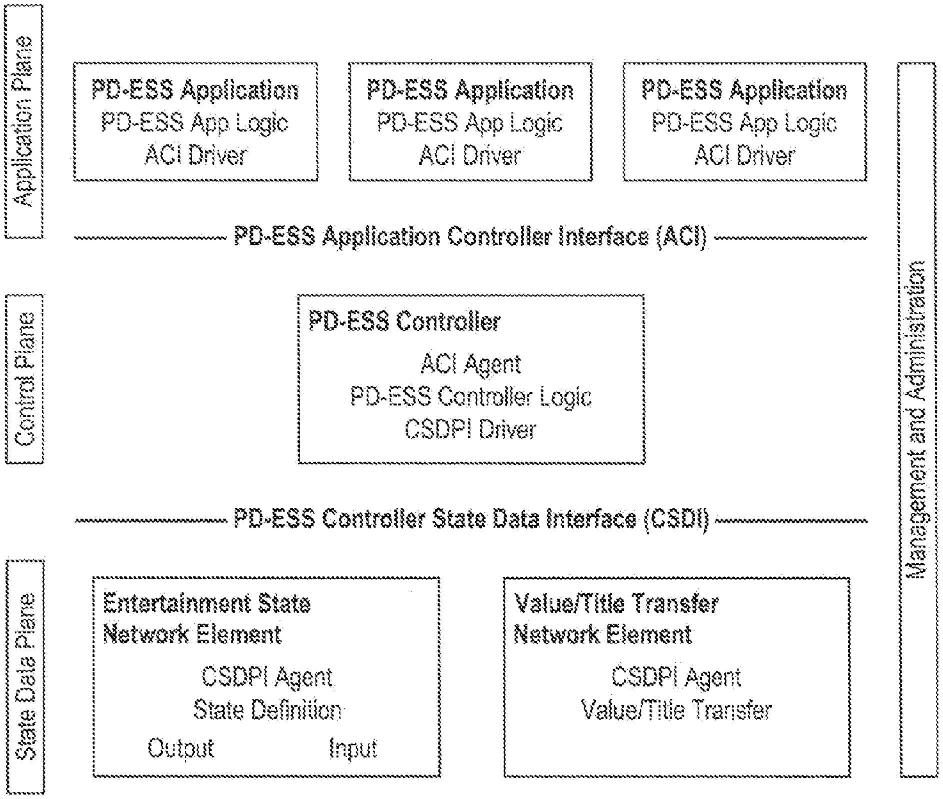
G06N 3/08	(2006.01)
G07F 17/32	(2006.01)
G06Q 20/06	(2006.01)
G06K 9/00	(2006.01)

(52) **U.S. Cl.**

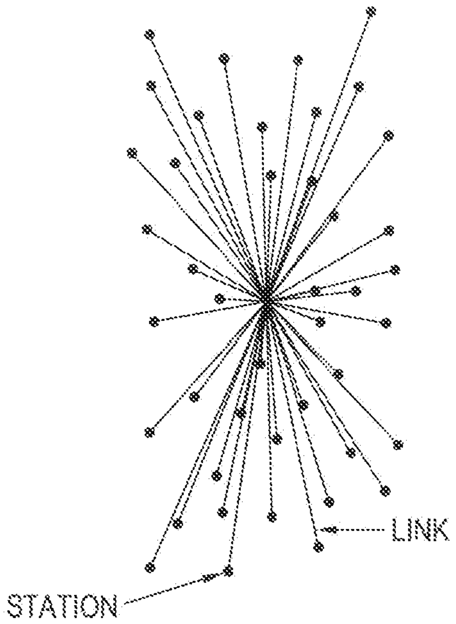
CPC ***G06N 3/08*** (2013.01); ***G07F 17/329*** (2013.01); ***G06K 9/00221*** (2013.01); ***G06Q 20/065*** (2013.01)

(57) **ABSTRACT**

In one aspect, the invention comprises a system for control of a transaction state system utilizing a distributed ledger. First, the system includes an application plane layer adapted to receive instructions regarding operation of the transaction state system. Preferably, the application plane layer is coupled to the application plane layer interface. Second, a control plane layer is provided, the control plane layer including an adaptive control unit, such as a cognitive computing unit, artificial intelligence unit or machine-learning unit. Third, a data plane layer includes an input interface to receive data input from one or more data sources and to provide output coupled to a decentralized distributed ledger, the data plane layer is coupled to the control plane layer. Optionally the decentralized distributed ledger stores data on cryptocurrency.



Programmatically Defined Gaming System

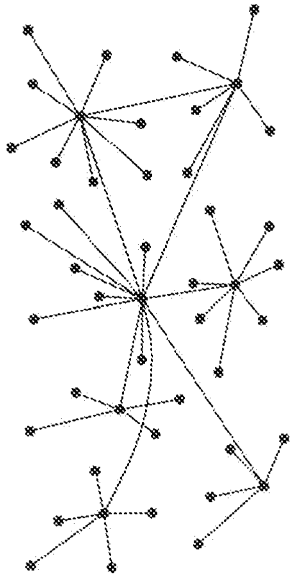


CENTRALIZED (A)

Prior Art Centralized System

FIG. 1

(Prior Art)

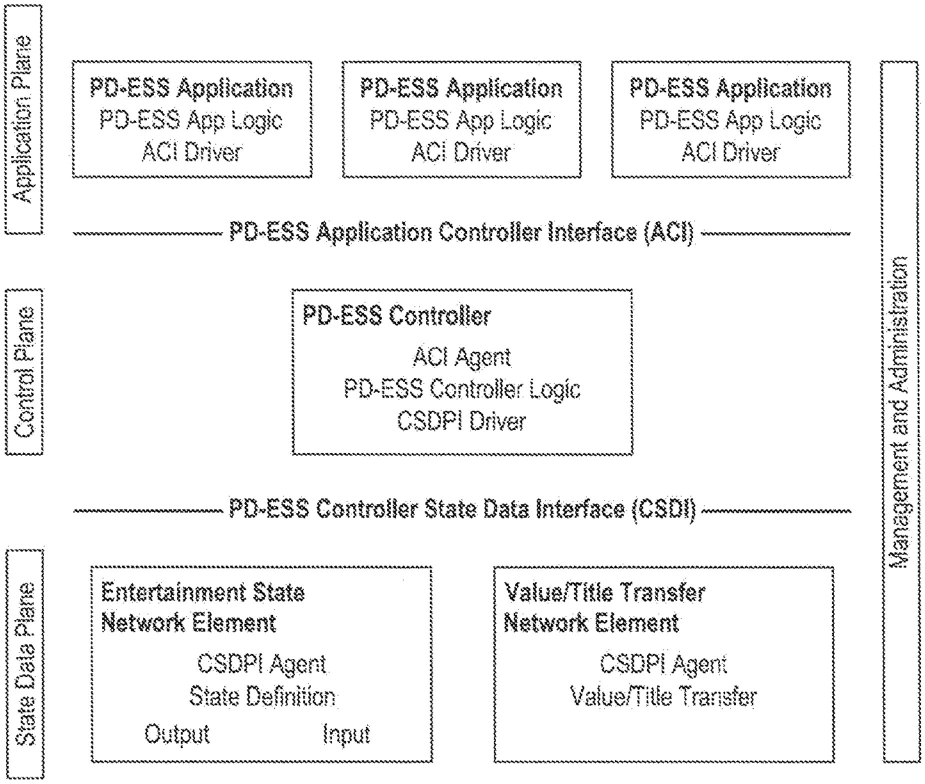


DECENTRALIZED

Prior Art Decentralized System

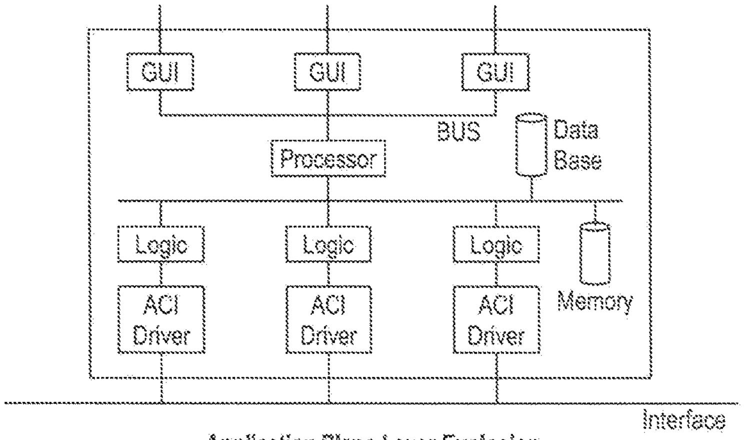
FIG. 2

(Prior Art)



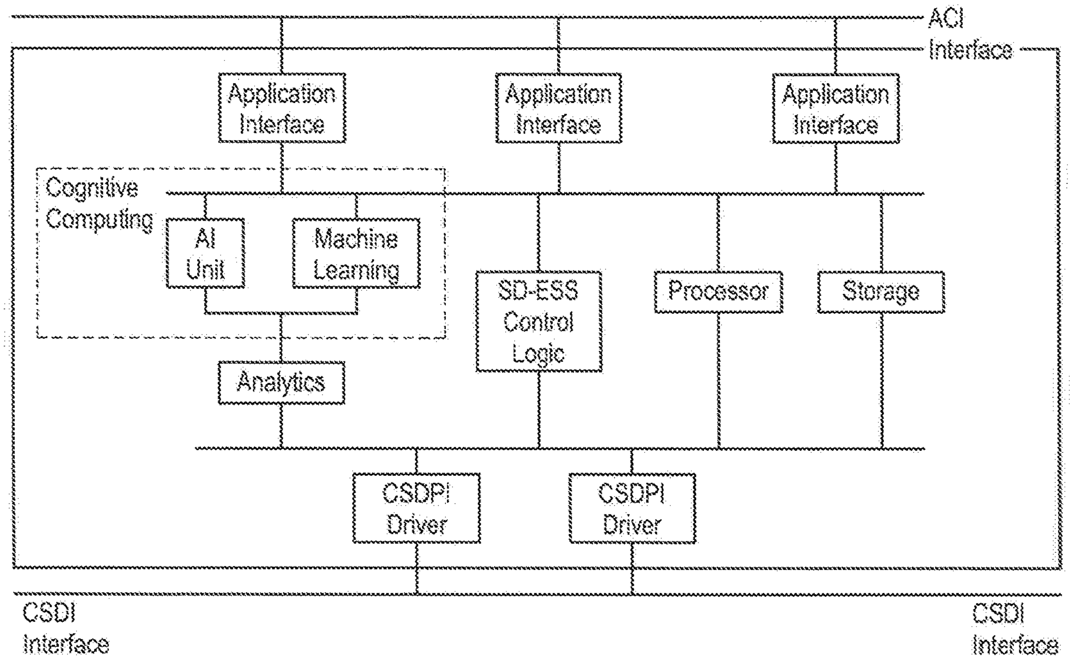
Programmatically Defined Gaming System

FIG. 3



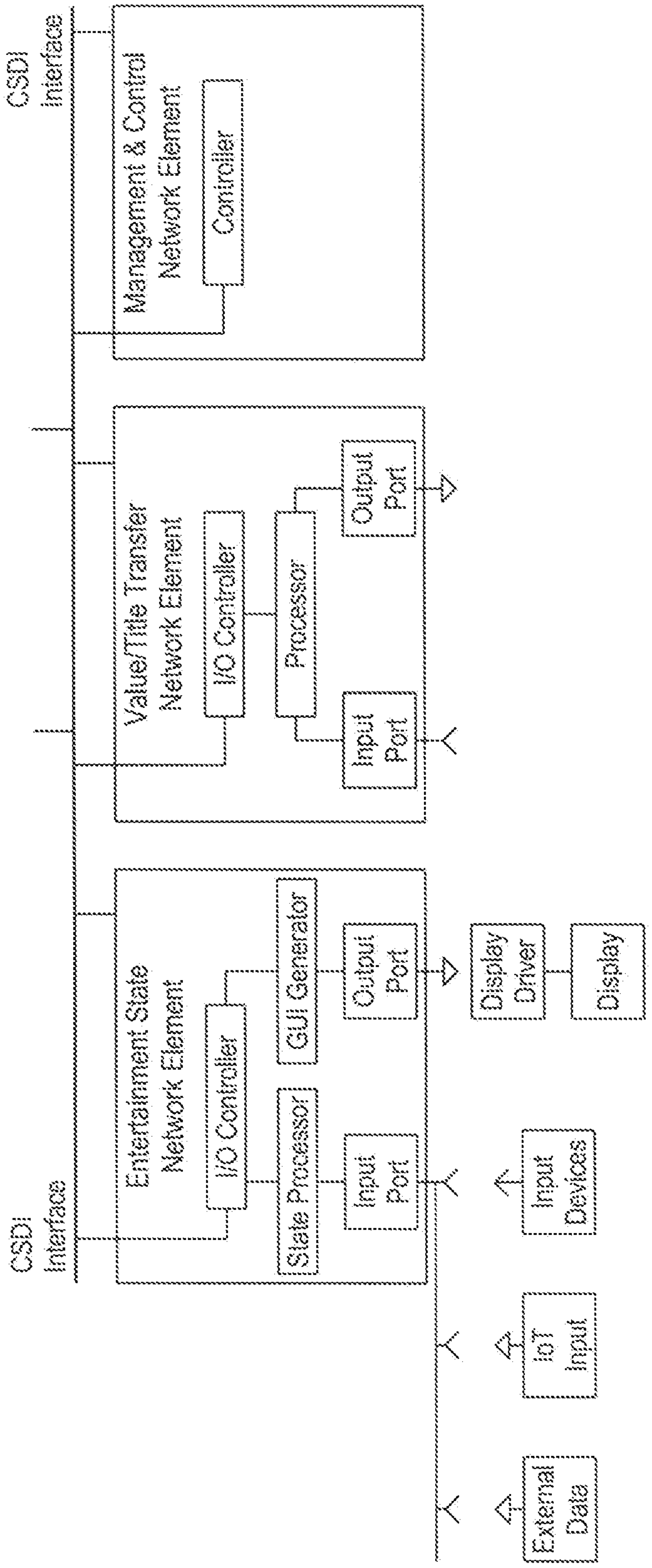
Application Plane Layer Explosion

FIG. 4



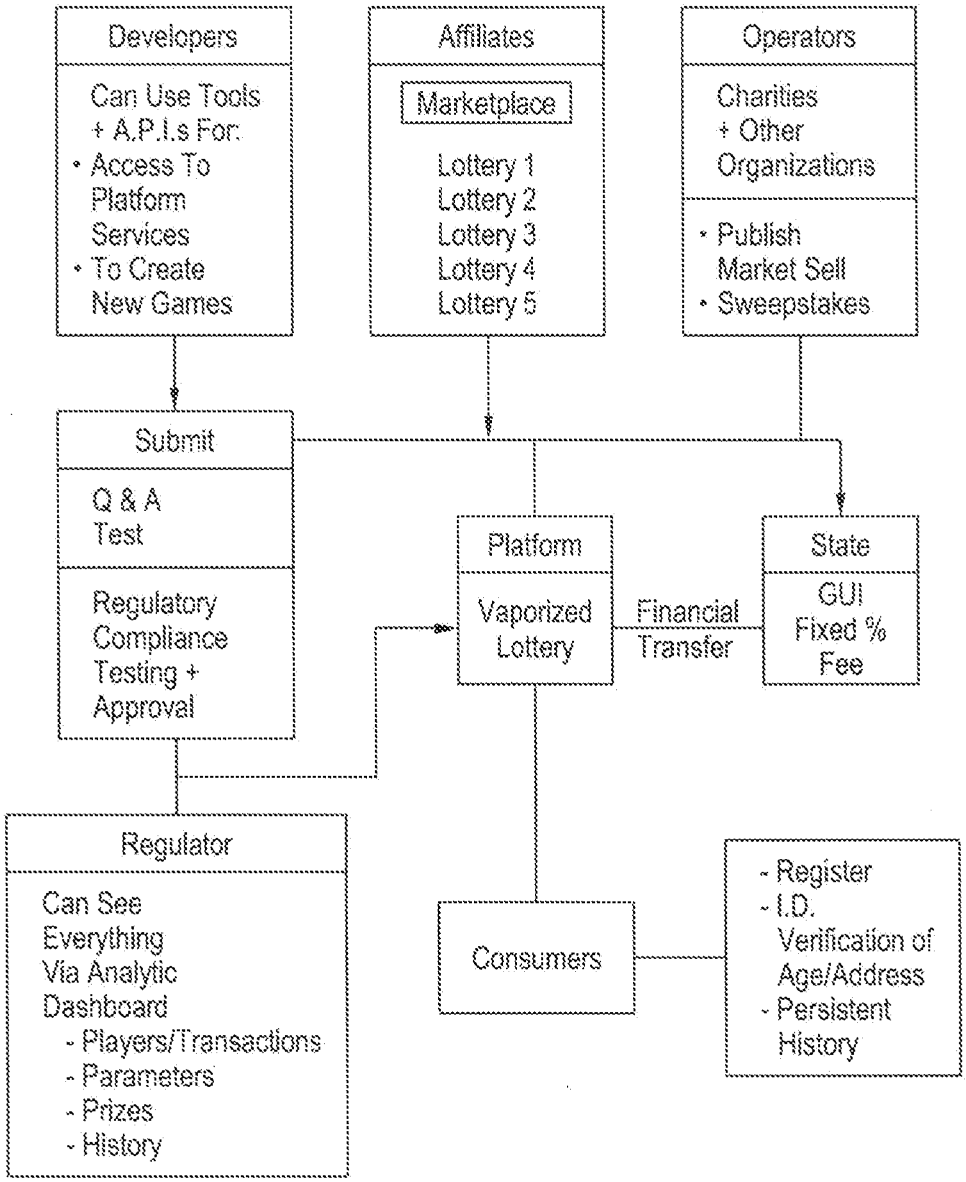
Control Plane Layer Explosion

FIG. 5



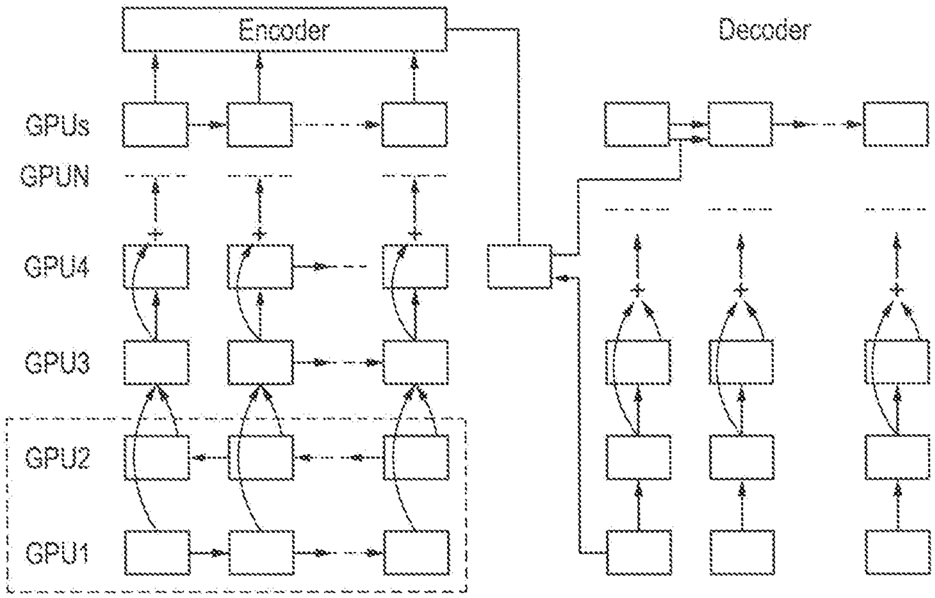
State Data Plane Layer Explosion

FIG. 6



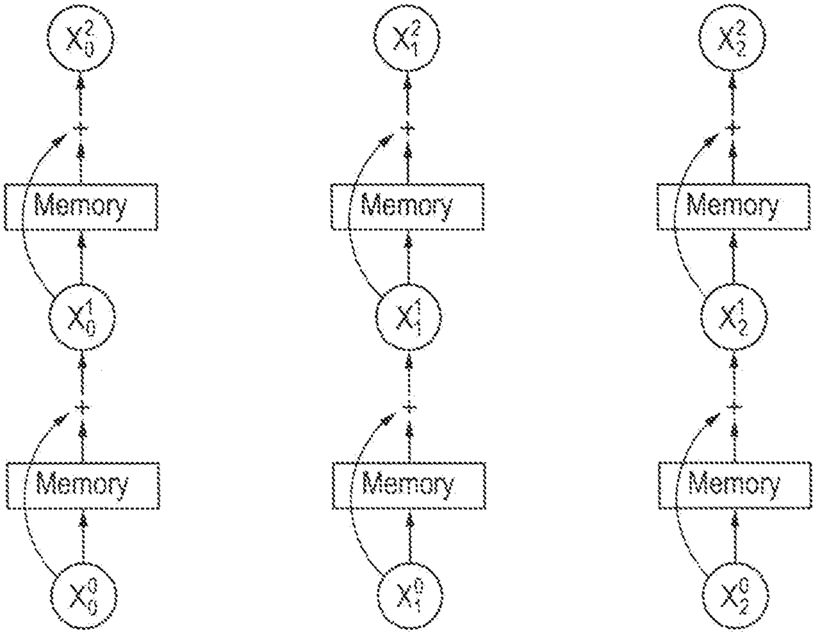
Ecosystem Interfaces and Interconnections

FIG. 7



Neural Network Model Architecture

FIG. 8



Neural Network

FIG. 9

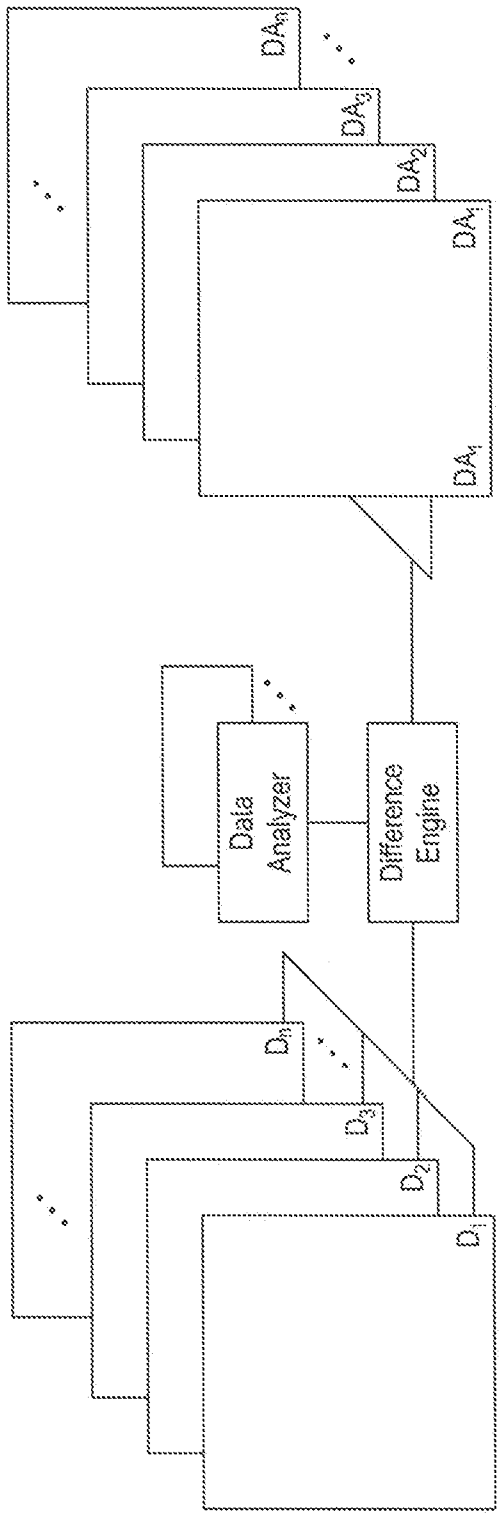

DA_n
DA_3
DA_2
DA_1
DA_1
Data Analyzer
Difference Engine
D_n
D_3
D_2
D_1

FIG. 10

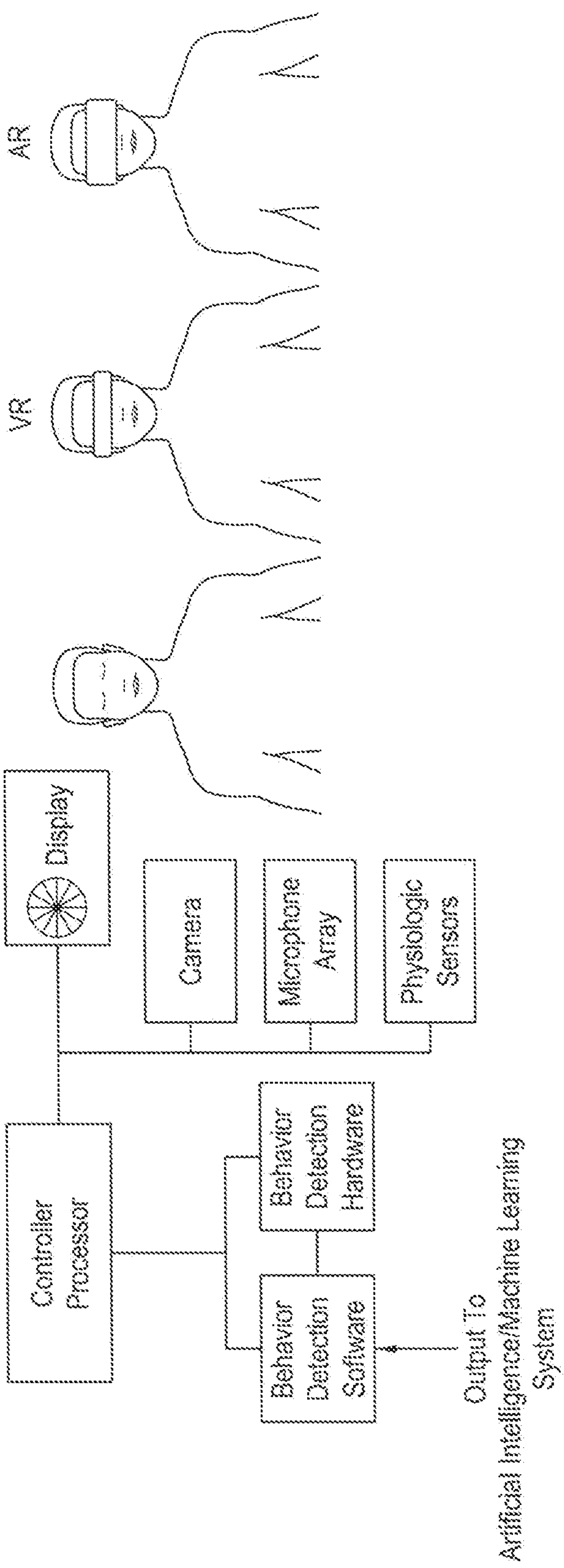
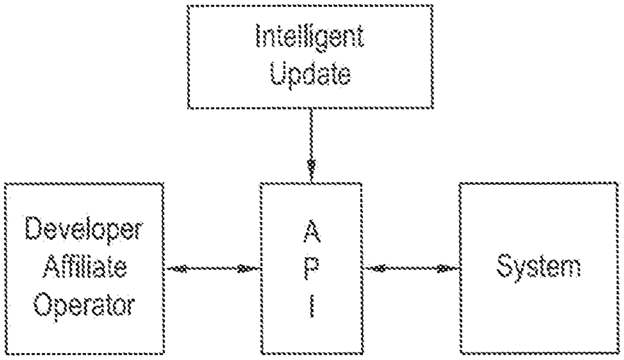
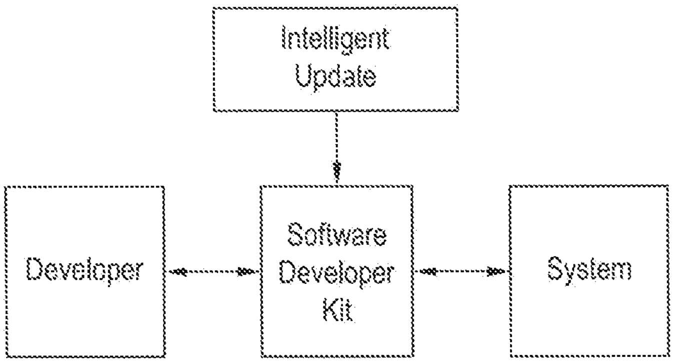

AR
VR
Display
Camera
Microphone Array
Physiologic Sensors
Controller Processor
Behavior Detection Hardware
Behavior Detection Software
Output To Artificial Intelligence/Machine Learning System

FIG. 11



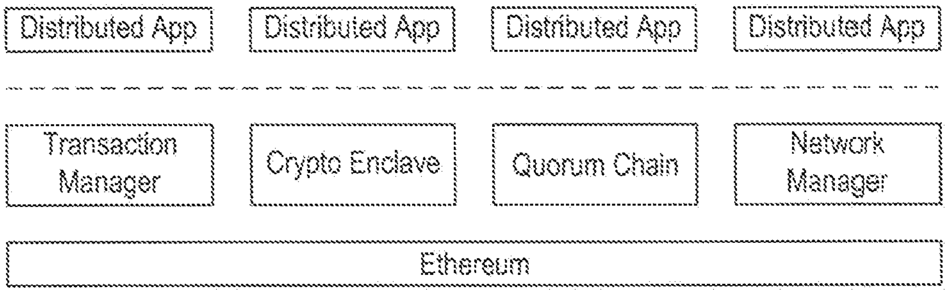
Dynamic Systems d-API

FIG. 12



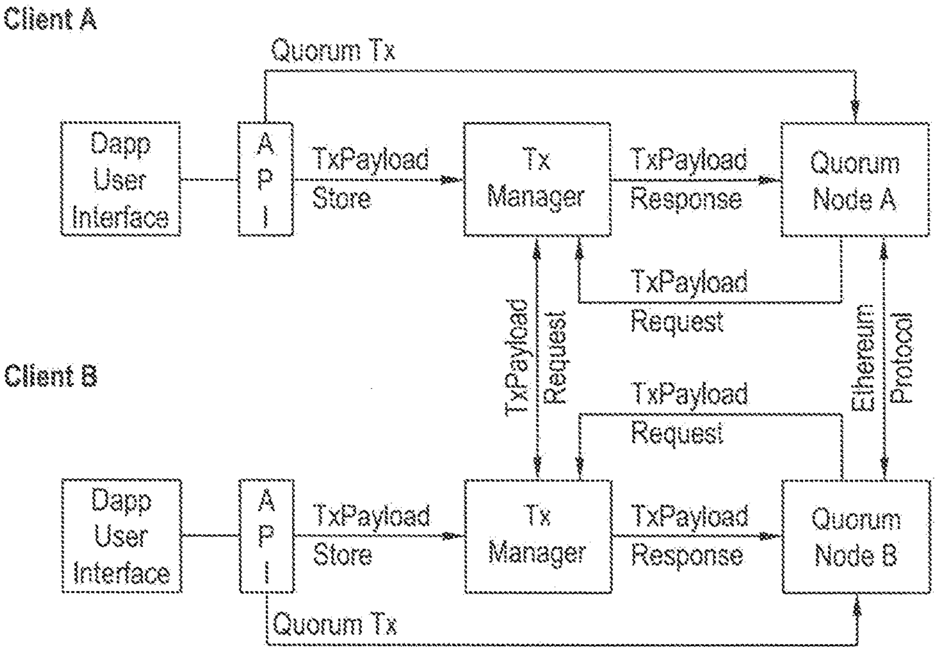
Dynamic Systems d-SDK

FIG. 13



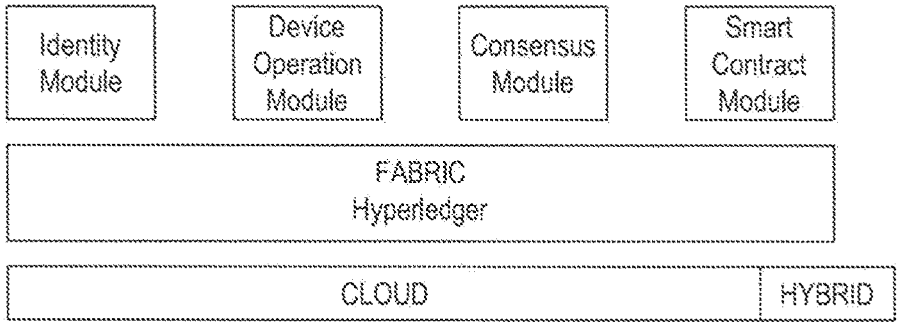
Architecture

FIG. 14



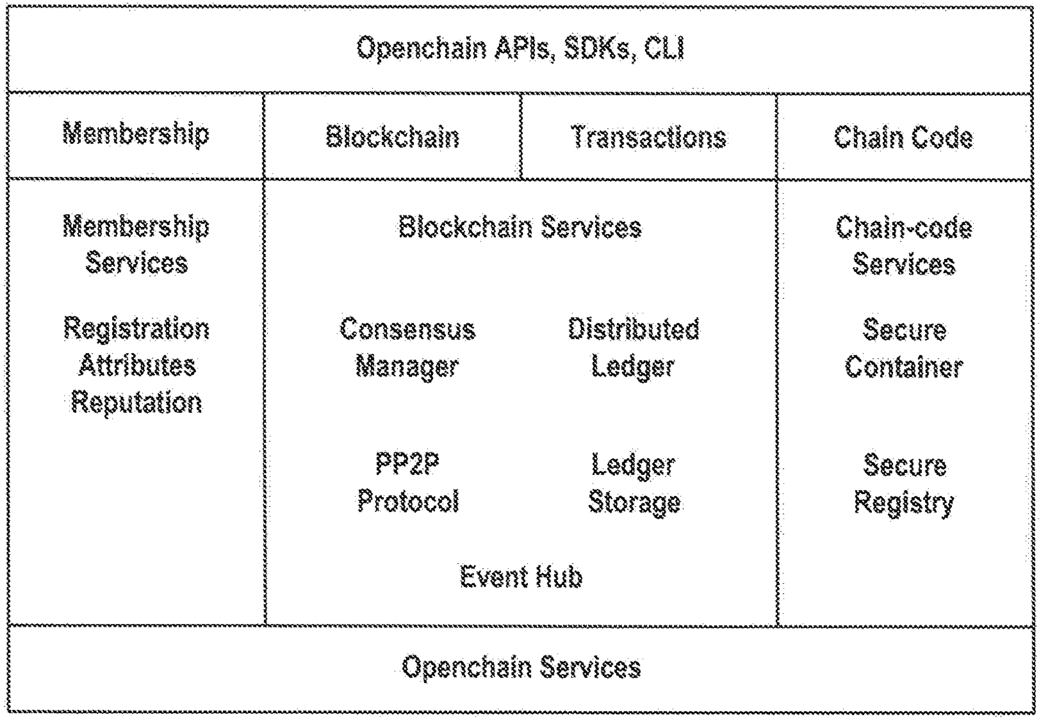
Permissioned System

FIG. 15



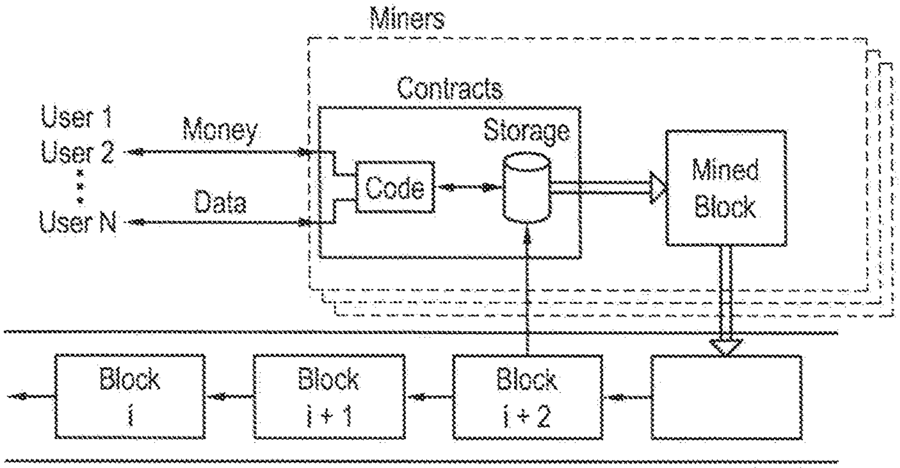
Blockchain Platform

FIG. 16



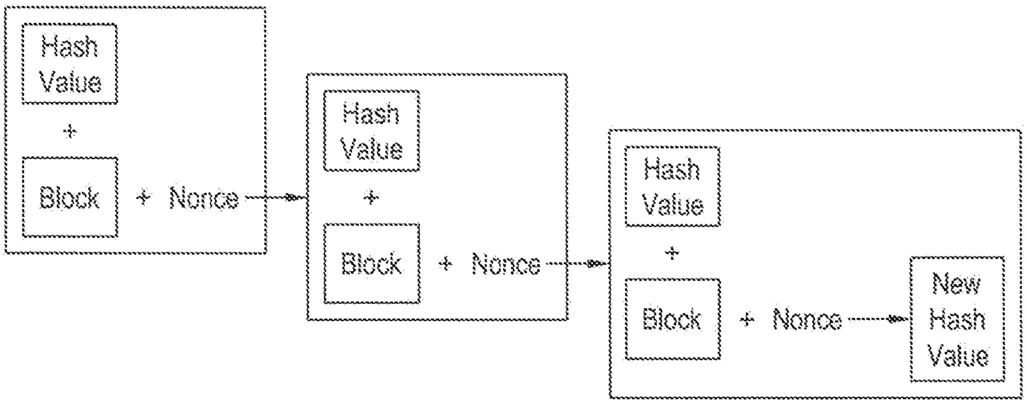
Platform

FIG. 17



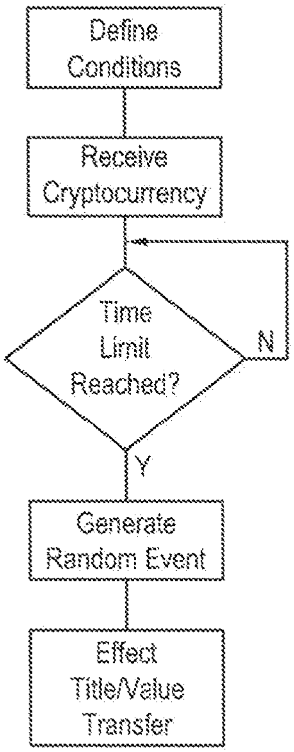
Schematic of a Decentralized Cryptocurrency System with Smart Contracts

FIG. 18



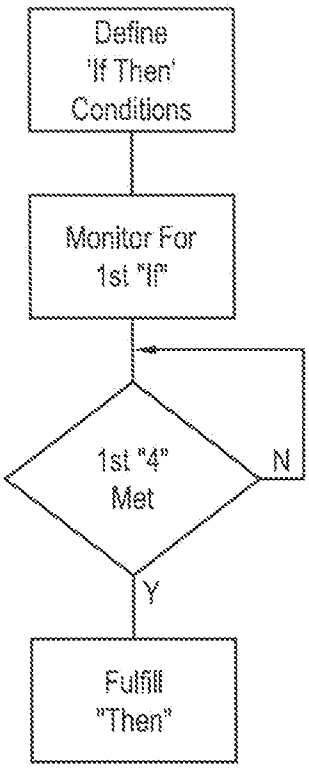
Schematic of Sequential Hash Value Creation
(Hash Value Plus Block Plus Nonce -> New Hash Value)

FIG. 19



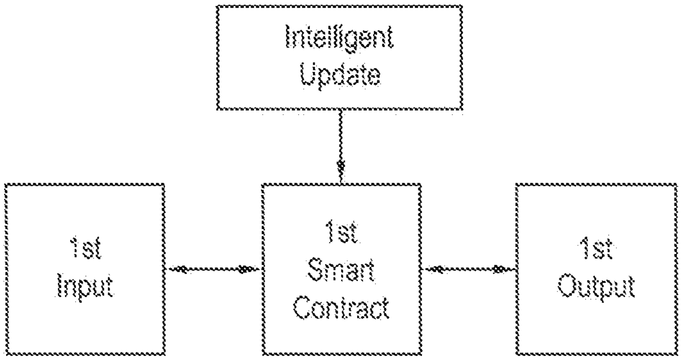
Flowchart for Crypto Currency Lottery

FIG. 20



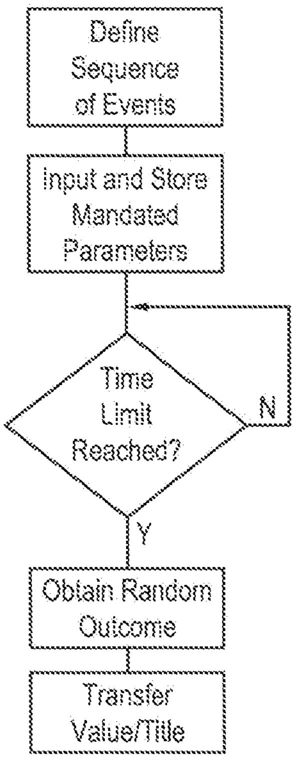
Smart Contract

FIG. 21



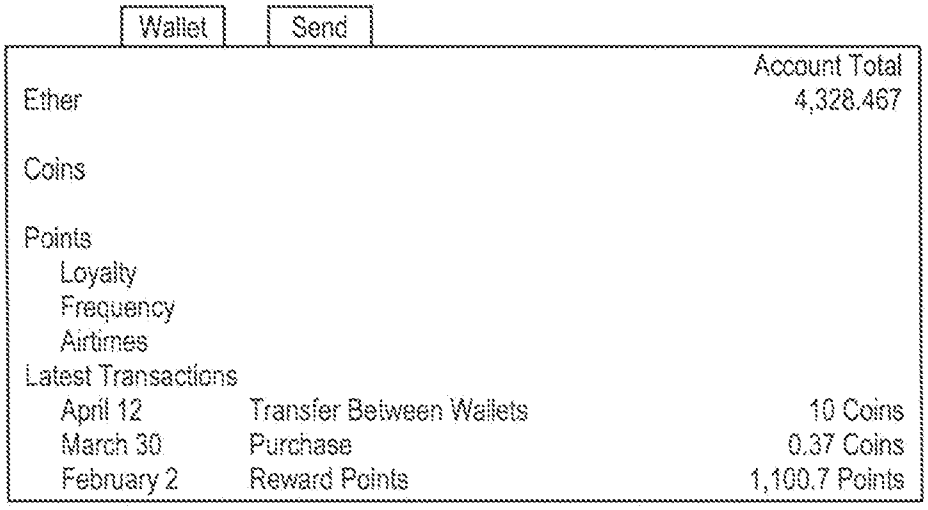
Smart-Smart (Smart^2) Contracts

FIG. 22



Smart Contracts with Mandated and Variable Parameters

FIG. 23



Account Total

Ether 4,328.467

Coins

Points

Loyalty

Frequency

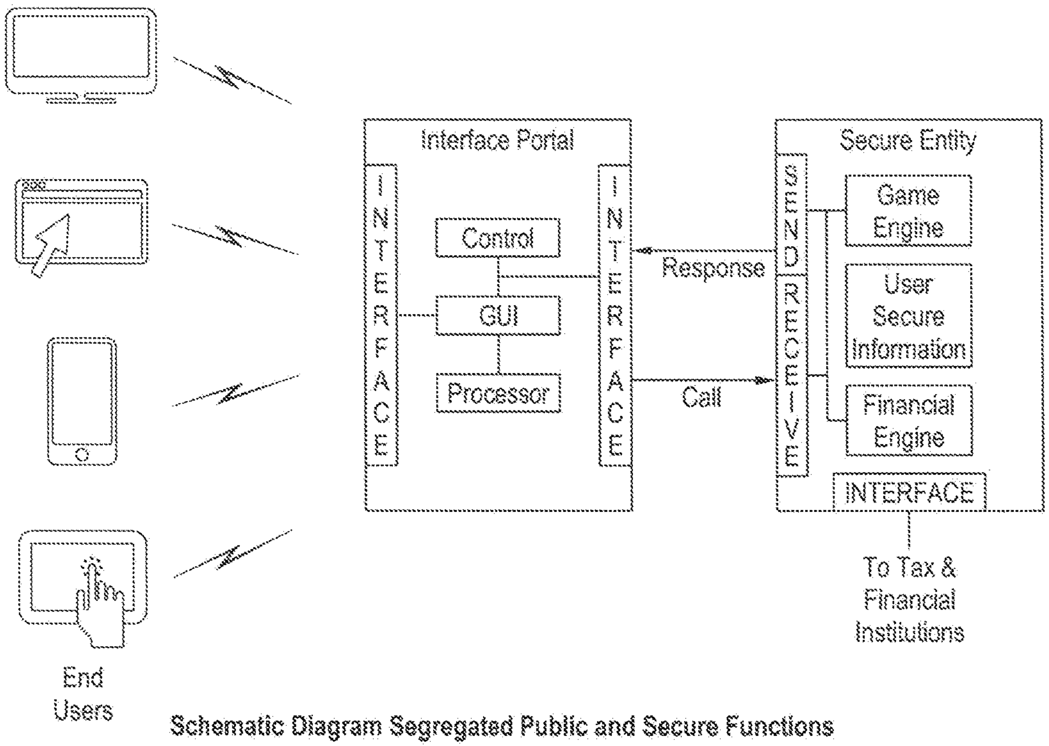
Airtimes

Latest Transactions

April 12	Transfer Between Wallets	10 Coins
March 30	Purchase	0.37 Coins
February 2	Reward Points	1,100.7 Points

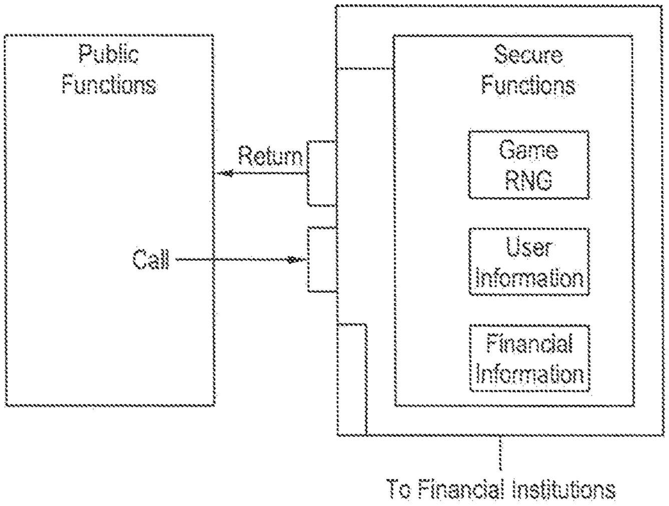
Cryptocurrency Wallet

FIG. 24



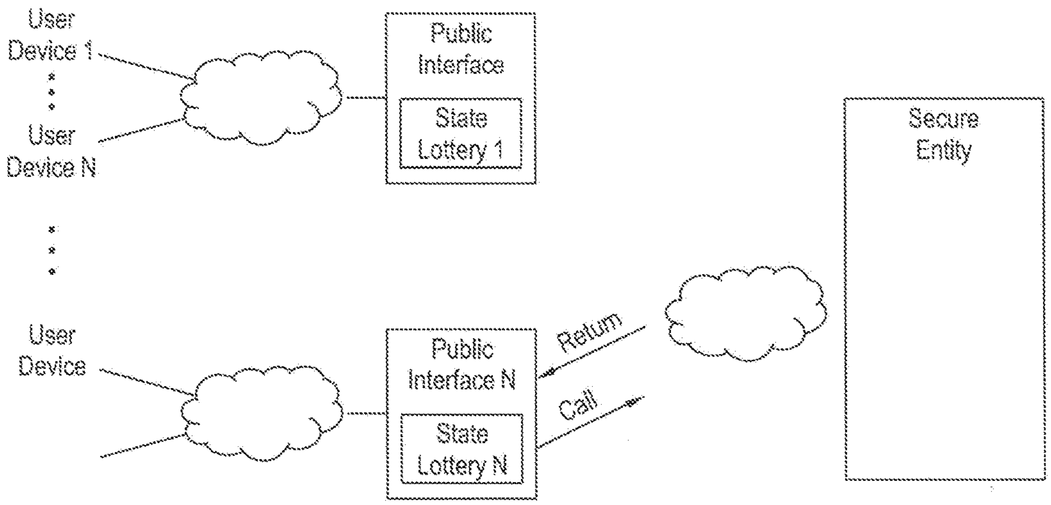
Schematic Diagram Segregated Public and Secure Functions

FIG. 25



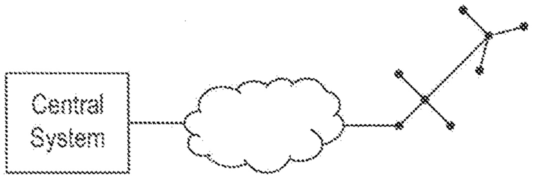
Interface of Segregated Secure and Public Functions

FIG. 26



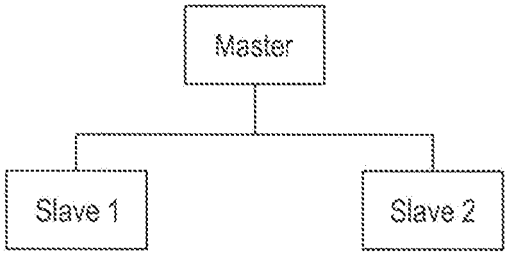
Network Implementation of Segregated Secure and Public Functions

FIG. 27



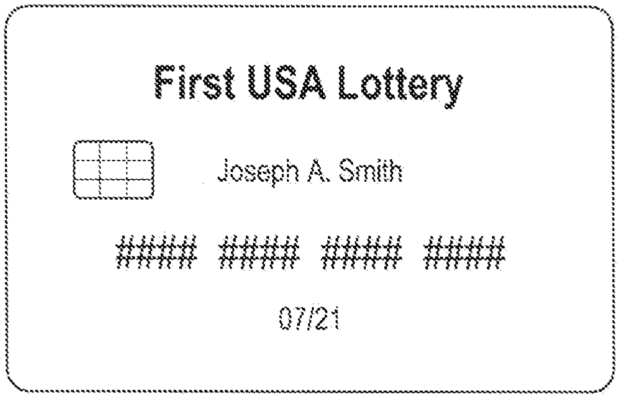
Centralized + Decentralized Systems

FIG. 28



Hierarchical Systems

FIG. 29



Lottery Linked Credit Card

FIG. 30

ARCHITECTURES, SYSTEMS AND METHODS FOR PROGRAM DEFINED TRANSACTION SYSTEM AND DECENTRALIZED CRYPTOCURRENCY SYSTEM

PRIORITY CLAIM

[0001] This is a continuation of application Ser. No. 15/886,432, filed Feb. 1, 2018, which claims benefit of provisional Application No. 62/454,423, filed Feb. 3, 2017, which are incorporated herein by reference as if fully set forth herein.

FIELD OF THE INVENTION

[0002] The present inventions relate to architectures, systems and methods for programmatically controlled entertainment state systems. More particularly, architectures, systems and methods for program control utilizing cognitive computing, including but not limited to artificial intelligence and machine learning, and optionally including analytics. Systems, methods and architectures are provided for game and entertainment operations are provided utilizing decentralized systems, including blockchain, optionally in peer to peer systems. More particularly, systems and methods for implementing a lottery, game or entertainment utilizing cryptocurrency, such as bitcoin, in a decentralized system.

BACKGROUND OF THE INVENTION

[0003] History shows that many trusted systems have evolved in order to provide for efficient functioning of society and business. Generally, these have involved central control of systems in order to ensure compliance with rules. Within the gaming space, examples include lotteries and regulated gaming. By way of example, the Nevada Gaming Control Board monitors institutions within the state for compliance with laws and regulations, and ensures the fair and efficient functioning of the industry.

[0004] Consider the entertainment and gaming system background. A lottery is a 'State' Function and serves as a form of 'trusted agent'. The classic definition of the elements of a lottery are prize, chance and consideration. When these elements are reordered into a more chronologically correct order, namely first, receipt and holding of the consideration (e.g., ticket purchases), chance (e.g., ensuring a fair and accurate random number generator) and prize (i.e., paying the prize to the true winner.) Therefore, the State acts as a 'trusted agent' as it holds the consideration, guarantees randomness of the 'chance', and pays out the prize (title transfer). 'Trust' is based on the Integrity and Trustworthiness of People Operating the System and the Regulators Who Oversee the System. Lotteries or State Regulators are often former law enforcement. The degree of trust in the Regulators is often based on time and track record, e.g., the State of Nevada Regulatory system is considered highly trustworthy and effective, based in part on a multi-decade long track record. Additionally, a State with the most business to lose from a loss of trust in the regulatory process is most motivated to provide regulation. Such systems are based on central control of the system.

[0005] A casino is a 'state regulated' function and a form of 'trusted agent' with 'verification'. They are licensed by the State and subject to state inspection.

[0006] Various advancements have been made in the gaming and entertainment environment. The following are assigned to the assignee of this, and are hereby incorporated by Reference as if fully set forth herein: Games, And Methods For Improved Game Play In Games Of Chance And Games Of Skill, U.S. Pat. No. 6,565,084, Games, and Methods and Apparatus for Game Play in Games of Chance, U.S. Pat. No. 6,488,280, Games, and Methods and Apparatus for Game Play in Games of Chance, U.S. Pat. No. 6,811,484, Apparatus and Method for Game Play in an Electronic Environment, U.S. Pat. No. 8,393,946, Apparatus, Systems and Methods for Implementing Enhanced Gaming and Prizing Parameters in an Electronic Environment, U.S. Pat. No. 7,798,896, Apparatus, Systems and Methods for Implementing Enhanced Gaming and Prizing Parameters in an Electronic Environment, U.S. Pat. No. 8,241,110, Methods and Apparatus for Enhanced Play in Lottery and Gaming Environments, U.S. Pat. No. 8,727,853, Methods and Apparatus for Enhanced Interactive Game Play in Lottery and Gaming Environments, U.S. Pat. No. 8,241, 100, Method and System for Electronic Interaction In A Multi-Player Gaming System, U.S. Pat. No. 8,535,134. Generally, they comprise a suite of tools to make systems more engaging, and to optimize results.

[0007] One vexing problem in larger systems results from systems incompatibility. Various components often come from various vendors. There is often a lack of interoperability and incompatibility. Various systems in the gaming ecosystem need to interoperate, including but not limited to: gaming operations, marketing, CRM (Customer Relationship Management), loyalty programs, Ancillary Points or Credits, System Analytics and Optimization, and account and audit functions.

[0008] Software Defined Systems are a collection of modules interoperated under a higher level of software control. These manage network services through abstraction of lower level functionality. Generally, there is an Application Plane, a Control Plane and a Data Plane. Examples include Software Defined Networks having a Control Plane which provides intelligent control of data plane composed of relatively less intelligent switches, routers, storage. Yet another example is software defined radio. The control plane monitors and supervises use of frequency bands in the data plane.

[0009] Yet another component is the use of static interfaces and tools. For example, APIs or Application Programming Interfaces generally comprise a static interface. They define a format for an information request. 'If you ask for X in a specific way, we will provide Y'. Generally, no access is provided by requestor to the system other than via API. Yet another system are SDKs or Software Development Kit. They may be static. Tools are provided to achieve desired results. GDKs or Game Development Kit also may be static and provide tools for game development.

[0010] The design of entertainment or games is often driven by metrics driven design. This often involves A/B Testing comparing the results or favorability as between multiple systems. Further, they often monitor multivariate response systems.

[0011] One aspect of lotteries and Lotto style games is that they tend to be static. At the most extreme example, they are literally printed on cardstock. More generally, once a format for a lottery game has been chosen, such as a 6 out of 49 format, it is difficult to change. Public perception of change is that the game has become less favorable to the player.

[0012] Problem gambling issues have plagued the gaming industry. It is a significant issue for society. While users can solicit help (e.g., 1-800-Gambling), there is often denial and an unwillingness to seek help. Various attempts have been made to limit abuse, such as use rate limits in some on-line games.

[0013] In the move from bricks and mortar to on-line and cyber spheres, identity issues proliferate. Issues include: are you who you purport to be and will the user's identity be compromised?

[0014] Significant advances have been made in cognitive intelligence and adaptive intelligence. For example, IBM Watson won a Jeopardy competition 2011 against highly skilled players. Deep learning and pattern recognition has occurred. Current trends include big data, pattern recognition and machine learning.

[0015] Recent advances have also been made in object detection, both in 2D and 3D space. A challenge in the Large Scale Visual Recognition Challenge (LSVRC) provides for Object Detection in ImageNet 2016. The error rate of automatic labeling of ImageNet declined to less than 3%, compared to human performance of about 5%.

[0016] Significant advances have also been made in machine based game play performance. In 2015, Google DeepMind used an artificial intelligence reinforcement learning system to learn how to play 49 Atari games. In 2016, AlphaGo system from Google DeepMind beat one of the world's greatest Go players 4-1. In 2017, Carnegie Mellon University's Libratus program defeated top human players in a statistically significant manner.

[0017] Further advances have been made in cloud based systems. Functions have been migrating from local servers and storage to remote 'cloud' storage. These systems provide for easy scalability. Clouds based systems may run multiple 'instances' simultaneously. They also may combine software as a service, including Artificial Intelligence ("AI").

[0018] The Internet of Things ("IoT") utilizes devices capable of sending data to remote location, and receiving command data. Various voice controlled devices use AI or machine learning ("ML"), e.g., Amazon Alexa, Google Dot.

[0019] FIG. **1** shows an exemplary prior art centralized system. FIG. **2** shows an exemplary prior art distributed system.

[0020] Advancements have been made in trusted distributed systems such as in the use of blockchain based systems. The initial disclosure of the blockchain technology is attributed to Satoshi Nakamoto in a paper published October, 2008. This system provides for automatic trust or system trust. The blockchain paradigm provides for a decentralized system utilizing decentralized consensus. This can be done in a peer-to-peer manner without an intermediary. The system may be viewed as a network of nodes running software on a programmable distributed network. It is sometimes referred to as a transaction singleton machine with shared state, a transaction based state machine, a message passing framework, a trustful object messaging compute framework and trusted computing.

[0021] A decentralized consensus is established by a combination of blockchain and cryptography. Authority and trust is provided by the decentralized virtual network. Consensus logic is generally separate from the application. It may comprise the first layer of a decentralized architecture.

[0022] Blockchain utilizes a distributed ledger. A 'block' comprises a new group of accepted transactions. A batch of transactions is released in a block to be validated by the network of participating computers. Continuous, sequential transaction record on a public block creates a unique "chain" or blockchain. This block is published to all other nodes. The publication occurs periodically, e.g. every 10 minutes.

[0023] Etherium is an open source platform for smart contracts. As currently operated, Etherium is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference. The applications run on a custom built blockchain, an extremely powerful shared global infrastructure that can move the value and represent ownership of the property. This allows developers to create markets, store debt or promise records, move funds according to long-standing instructions (such as a will or a futures contract), without the counterparty risk. Etherium also states that its goal is to create a tradeable digital token that can be used as a currency, a representation of an asset, a virtual share, a proof of membership or anything at all. These tokens use a standard coin API, so the contract will be automatically compatible with any wallet, other contract or exchange also using this standard. The total amount of tokens in circulation can be set to a simple fixed amount or fluctuate based on any programmed ruleset. In summary, Etherium states that it enables building a tradeable token with a fixed supply, a central bank that can issue money and a puzzle-based cryptocurrency.

[0024] There are many disadvantages to the current systems. They are slow to change and innovate. They often involve proprietary systems that do not interoperate. There is often governmental and or institutional bias. There may be a cumbersome regulatory environment. Finally, there are often high transaction costs.

[0025] Thus, there is a need for interoperability among inconsistent, often proprietary systems. There is a need for gambling limitation on a more global basis, including geo-limitation and global use rate monitoring for problem gambling. There is a need for problem gambling detection and remediation. There is a need for improved distributed systems.

SUMMARY OF THE INVENTION

[0026] In one aspect, the invention comprises a system for control of a transaction state system utilizing a distributed ledger. First, the system includes an application plane layer adapted to receive instructions regarding operation of the transaction state system. Preferably, the application plane layer is coupled to the application plane layer interface. Second, a control plane layer is provided, the control plane layer including an adaptive control unit, such as a cognitive computing unit, artificial intelligence unit or machine-learning unit. Third, a data plane layer includes an input interface to receive data input from one or more data sources and to provide output coupled to a decentralized distributed ledger, the data plane layer is coupled to the control plane layer. Optionally the decentralized distributed ledger stores data on cryptocurrency.

[0027] Systems and methods are provided for training an artificial intelligence system including the use of one or more human subject responses to stimuli as input to the artificial intelligence system. One or more displays are oriented toward the human subjects to present the stimuli to the human subjects. One or more detectors serve to monitor the reaction of the human subjects to the stimuli, the detectors including at least motion detectors, the detectors providing an output. An analysis system is coupled to receive the output of the detectors, the analysis system providing an output corresponding to whether the reaction of the human subjects was positive or negative. A neural network utilizes the output of the analysis system to provide a positive weighting for training of the neural network when the output of the analysis system was positive, and a negative weighting for training of the neural network when the output of the analysis system was negative.

BRIEF DESCRIPTION OF THE DRAWINGS

[0028] FIG. **1** is a diagrammatic view of a prior art centralized system.

[0029] FIG. **2** is a diagrammatic view of a prior art centralized system.

[0030] FIG. **3** is a system level block diagram of the program defined entertainment state system (PD-ESS) showing the application plane, the control plane and the state data plane.

[0031] FIG. **4** is a system level block diagram explosion of the application state plane layer of the PD-ESS.

[0032] FIG. **5** is a system level block diagram explosion of the control plane layer of the PD-ESS.

[0033] FIG. **6** is a system level block diagram explosion of the state data plane layer of the PD-ESS.

[0034] FIG. **7** is a diagrammatic view of the ecosystem, including interfaces and interconnections.

[0035] FIG. **8** is a system level block diagram of the neural network model architecture including graphical processing units (GPUs).

[0036] FIG. **9** is a system level block diagram of the neural network model architecture.

[0037] FIG. **10** is a system level diagram of multiple data sets including a difference engine and data analyzer.

[0038] FIG. **11** is response system display and detection system for generating input to train the artificial intelligence (AI) and machine learning (ML) systems.

[0039] FIG. **12** is a system level diagram of a dynamic system application programming interface (d-API).

[0040] FIG. **13** is a system level diagram of a dynamic software development kit (d-SDK).

[0041] FIG. **14** is a system architecture level diagram of a distributed system including blockchain and Etherium.

[0042] FIG. **15** is a system architecture level diagram of a permissioned blockchain system.

[0043] FIG. **16** is a system architecture level diagram of a blockchain platform.

[0044] FIG. **17** is a system architecture level diagram of a blockchain platform including open chain services.

[0045] FIG. **18** is a system architecture level diagram of a decentralized cryptocurrency system with smart contracts.

[0046] FIG. **19** is a system architecture level diagram of a decentralized system with sequential hash value creation.

[0047] FIG. **20** is a flowchart diagram of a cryptocurrency lottery.

[0048] FIG. **21** is a flowchart diagram of a smart contract.

[0049] FIG. **22** is a flowchart diagram of a smart-smart (smart^2) contract.

[0050] FIG. **23** is a flowchart diagram of a smart contract having mandated and variable parameters.

[0051] FIG. **24** is a graphical user interface (GUI) of a cryptocurrency wallet.

[0052] FIG. **25** is a system architecture level schematic diagram of a system having segregated public and secure functions.

[0053] FIG. **26** is a system architecture level of an interface of segregated public and secure functions.

[0054] FIG. **27** is a system architecture level of a network implementation of a system having segregated public and secure functions.

[0055] FIG. **28** is a system architecture level of a combined centralized and decentralized system.

[0056] FIG. **29** is a system architecture level of a hierarchical system.

[0057] FIG. **30** is a plan view of a lottery linked credit card.

DETAILED DESCRIPTION OF THE INVENTION

[0058] Architectures, Systems and Methods for Program Defined Entertainment State Systems.

[0059] The following description is primarily in connection with FIGS. **3**, **4**, **5** and **6**, but may apply to other figures as well. An architecture is provided for a program defined entertainment state system. This preferably serves to decouple the system that controls the overall experience from the underlying systems that define states. The first plane, the application plane provides an interface, primarily for system side users, e.g., developers, organizers of events, contests, lotteries. The second plane, the control plane, provides for intelligent control, especially cognitive computing, including artificial intelligence and/or machine learning, including artificial intelligence where the system learns over time. This preferably provides an intelligent control layer above modules. The third plane, the state data plane, provides for entertainment 'state modules' with various mechanics, preferably including 'core loop', meta states and provides interfaces for end users, as well as inputs and outputs.

[0060] FIG. **3** provides a block Diagram Program Defined Entertainment State System (PD-ESS). FIG. **4** is an Explosion of PD-ESS Application Plane Layer, including an application layer GUI (facing the Developers, Affiliates, and Charities). FIG. **5** provides an Explosion PD-ESS controller plane layer. FIG. **6** provides an explosion PD-ESS state data plane layer. Also included are an explosion of entertainment state network element layer, a user interface GUI, an explosion of value/title transfer network element and explosion of other functional blocks.

[0061] Turning first to the Application Plane Layer, a program serves to communicate requirements and desired behavior to the PD-ESS Controller. It provides communication between the PD-ESS Application and PD-ESS Controller via the PD-ESS Application Controller Interface (ACI). Application Logic and Drivers are optionally provided. The application layer may receive an abstracted view of State Data Plane Actions. The PD-ESS Applications may interface with higher levels of abstracted control. The system includes an interface, the PD-ESS Application Controller Interface (ACI). The management and administration preferably provides the following: (1) To/From Application Plane, it provides contracts and SLAs, (2) To/from Control

Plane Configure Policy, Monitor Performance, and (3) To/From Data Plane Element Setup.

[0062] Turning second to the Control Plane Layer, the PD-ESS Controller is ideally logically centralized entity, preferably serves to translate the requirements of the PD-ESS Application to the State Data Plane layer, and provides the Application layer with actions in the State Data Plane (e.g., event information and statistical information). The control plane may provide statistics, events and states from the Data Plane to the Application Plane. The control plane preferably enforces behavior at a low level control in the data plane, provides capability discovery, and monitors statistics and faults. The control plane advantageously includes cognitive computing, such as artificial intelligence (AI) and machine learning (ML), to be described in greater detail, below.

[0063] The control plane may optionally include analytics, including but not limited to pattern recognition. Analytics may be performed on a population, preferably a relevant population, or on a subset. Preferably, the subset has similar characteristics of a target user. Data may be binned according to subset. The scope of primary data may be analyzed. Predictive modeling may be included. Responsible Gaming Control may be implemented at the control plane level, especially if there are use rate limits and global limits.

[0064] Turning thirdly to the state data plane layer, it preferably includes main subcomponents and Functional Network Elements. Optionally, the functional network elements include some or all of the following: 1. Entertainment State Network Elements, 2. Value/Title Transfer Network Element, 3. Game Library, such as Casino, VLT, Video Gaming, Tournament, Amusement with Prize (AWP), Game Mechanics, Core Loop, Skill, Skill with Reveal, Second Chance, Social, Gamification, Prizing, vGLEPs and Prize Board, 4. Systems, Marketing, Promotions, CRM, Operations, Logistics, Interactive, Mobile/Apps and Responsive Design, 5. Platforms, 6. Channels, 7. Lottery, including Retail and Central Systems, 8. Loyalty, 9. Responsible Gaming Control, optionally including use rate limits and global limits (may be done in the control plane layer as well), 10. Sports, including real world, fantasy and eSports, 11. Other Live Data Entertainment, 12. Networks, including Network communications and web services and 13. Management, including Records, Player Account Management, Reporting, Compliance, including regulatory compliance, security, including cybersecurity, fraud and risk management, including preferably audit and payment.

[0065] The Entertainment State Network Elements provide an interface for interaction with a user of the system. An input receives information from user selection. Sensors may be of various forms, including sound sensors, motion sensors, whether 2-d or 3-d, such as including the Microsoft Kinect system. ‘Internal Data’ consists of data related primarily to game operations. ‘External’ Data sources to combine with Primary Data Source. These may include 1. Location, 2. Current Activity such as Driving (provided by vehicle, provided by tracked phone) or Exercising (provided by FitBit or similar), 3. Economic Conditions, 4. Weather, 5. Recent Events/News, e.g., a recent Large PowerBall win, 6. Marketing Information, 7. e-mail scans, e.g., Google scanning of Gmail for content, 8. Social Media, and 9. the Internet of Things (IoT). The Internet of Things (IoT) provide various forms of connected devices such as data sensors. The sensors generate data input “stimuli” to system. By utilizing any form of input, the system is able to provide for massive parallelism. All data “stimuli” to system permits the system to be adaptive and reactive to all data stimuli.

[0066] An Output provides stimulation to user. Forms may include: 1. images, such on a display, or via a GUI, or VR system, AR system, 2. Thin Client display with remote computing power, 3. Projections and Holograms, 4. sounds, 5. tactile stimuli, 6. olfactory stimuli, or 7. direct electrical stimuli, neural or otherwise.

[0067] A Value/Title Transfer Network Element serves to receive and transfer value (money, coins, and other items of value). Value may refer to fungible liquid asset or other store of value. Title generally refers to ownership of real, personal, or virtual property. A detailed discussion of blockchain, trust-less, and cryptocurrency systems is provided, below.

[0068] Artificial Intelligence (AI) is broadly that branch of computer science dealing in automating intelligent behavior. They are systems whose objective is to use machines to emulate and simulate human intelligence and corresponding behavior. This may take many forms, including symbolic or symbol manipulation AI. It may address analyzing abstract symbols and/or human readable symbols. It may form abstract connections between data or other information or stimuli. It may form logical conclusions. Artificial intelligence is the intelligence exhibited by machines, programs or software. It is has been defined as the study and design of intelligent agents, in which an intelligent agent is a system that perceives its environment and takes actions that maximize its chances of success. Yet others have defined it as the science and engineering of making intelligent machines.

[0069] Artificial Intelligence often involves use of neural networks. In various embodiments, a multi-layer stack of neural network nodes are utilized. The lowest level comprises granular elements. By way of example in a gaming application, in the order of higher level understanding, the levels would progress from instances of individual action (granular), to core loop detection, to session play, to multi-session play. Optionally, a parsing engine serves to break down or subdivide a larger set, such as a data set or image, into more discrete or granular elements.

[0070] AI may have various attributes. It may have deduction, reasoning, and problem solving. It may include knowledge representation or learning. Systems may perform natural language processing (communication). Yet others perform perception, motion detection and information manipulation. At higher levels of abstraction, it may result in social intelligence, creativity and general intelligence. Various approaches are employed including cybernetics and brain simulation, symbolic, sub-symbolic, and statistical, as well as integrating the approaches.

[0071] Various tools may be employed, either alone or in combinations. They include search and optimization, logic, probabilistic methods for uncertain reasoning, classifiers and statistical learning methods, neural networks, deep feedforward neural networks, deep recurrent neural networks, deep learning, control theory and languages.

[0072] AI advantageously utilizes parallel processing and even massively parallel processing in their architectures. Graphics Processing Units (GPUs) provide for parallel processing. Current versions of GPUs are available from various sources, e.g., Nvidia, Nervana Systems.

[0073] Machine Learning is defined as a system that builds up knowledge from experience. Machine learning serves to detect patterns and laws.

[0074] Deep Learning uses Neural AI. It is easily scalable, and typically involves more layers or neural Networks (NNs). Neural Networks may be of various forms, including: efficient NN, vectorized NN, vectorized logistic regression, vectorized logistic regression gradient output, binary classification, logistic regression, logistic regression cost function, gradient descent, derivatives, computation graph and logistic regression gradient descent.

[0075] Deep neural networks (DNN) often involve hyperparameter tuning. Typically they utilize regularization and optimization. Sometimes they are referred to as Deep Belief Network (DBN).

[0076] Other forms of neural networks include Convolutional Neural Networks (CNN) or Recurrent Neural Networks (RNN). Examples of available systems include: LSTM, Adam, Caffe, Dropout, Batch Norm, Xavier/He, Python, Scikit-Learn and TensorFlow.

[0077] AI may operate on various forms of data sets. The data set may comprise images, whether video images, 2D Data and/or 3D Data. Sequential data may be analyzed. Examples include, but are not limited to, natural language, audio, autonomous driving decisions, game states and game decisions.

[0078] Various industry applications advantageously benefit from application of AI. They include imaging and object detecting, serving to identify, classify, mining and optionally provide sentiment analysis. Other applications include autonomous driving. Yet other applications include robots and robotics. Within healthcare, functions include imaging analysis, diagnosing and gamification. Various forms of sequential data analysis may be enhanced, such as speech recognition, and natural language processing. Music applications include both recognition and synthesis. Within the gaming field, applications include game state sequences detection, analysis, formation, combination optimization, and game optimization. Chat bots and machine translation advantageously employ these systems.

[0079] FIG. **7** shows the constituent function blocks within an entertainment or gaming ecosystem. Affiliates serve to acquire customers. Affiliates receive a commission, such as based on the number of users acquired or a percent (%) of revenue. Optionally, there is a link to a credit card function (to be discussed, below in connection with FIG. **30**).

[0080] Next are charities and other organizations that plan to operate a lottery, game or other entertainment event. They provide for customer acquisitions. They are the recipient of the event (game, lottery or entertainment). They also collect a fee.

[0081] Next are the developers, who provide for game design. In return for game design, they receive multi-jurisdictional use and payment for use. An enhanced application or app store may be provided wherein the game design may be viewed, selected and downloaded.

[0082] Next, consumers provide registration and identification information. The registration data may optionally include identification, age, address and verification. Optionally, the data is sufficient that the system can comply with Know Your Customer (KYC) rules, with optional levels of identity verification. This is stored as persistent history. The customer receives a chance to play, win, and receive entertainment.

[0083] Next is the regulator or trust verifying agent. They provide testing, approval for game fairness, overall approval, ensure compliance with regulations and security. The regulator or trust verifying agent is granted access permission by the system to monitoring of every transaction, (analytics dashboard), player accounts, parameters, prize amounts and payouts, and to the complete history. The regulator or trust verifying agent receives compensation, whether a fee or as a percentage of the transaction amounts.

[0084] Next, the lotteries serve as the trusted agent, and receive a percentage of the transaction amount. Optionally, the historical functions of the lottery may be eliminated or vaporized from the system when those functions are performed by another entity within the ecosystem.

[0085] FIGS. **8** and **9** relate to the learning processes for training neural networks. By providing repeated input stimulus and then training the neural network to provide the correct output, the system may be taught to form the correct associated output based on one or more input stimuli. In converting input to the desired output the training may comprise supervised learning, such as when the target values and parameters are supervised. Alternatively, the training may be non-supervised learning, wherein the system attempts to identify patterns in the input that have identifiable structure and can be reproduced. Alternately, the system may use reinforcement learning, which works independently (like non-supervised learning) but is rewarded or punished depending on success or failure. Preferably, reinforcement learning involves incremental change. In the various training techniques, perturbation may be used wherein one or more input parameters are varied, typically in a perturbation amount, e.g., less than 10%, more preferably less than 5%, and most preferably less than 3%, of the input value, so as to monitor the effect of the perturbation on the output.

[0086] Hyperparameters and parameters may be used in the AI or machine learning systems. Model parameters are estimated from data automatically. A configuration variable internal to the model can be estimated from data. This can be required by the model when making predictions. Values define the skill of the model. They may be estimated or learned from data.

[0087] Hyperparameters are set manually and are used in the processes to help estimate parameters. A configuration variable external to the model is used. Generally, it cannot be estimated from the data. They are often used in processes to estimate model parameters. They are typically specified by the system user. Hyperparameters can often be set using heuristics. They are often tuned for a given predictive modeling problem. A hyperledger may be used, either as a hyperledger composer or hyperledger fabric.

[0088] The AI or machine learning may be performed on various types of hardware. Advantageously, systems that support parallel processing can provide for computation speed and efficiency. Parallel processing units such as Graphics Processing Units (GPUs) are available from NVIDIA and AMD. Neural Processing Units (NPUs) are available in the Kirin **970**. Apple A11 and the Qualcomm Zeroth Processor. AI and machine learning processing is also available as a cloud AI or Machine learning system, such as is available from Google and Amazon Web Services.

[0089] FIG. **10** describes domain transformations and difference engines. One advantageous domain transformation involves the time domain to frequency domain (time series to frequency domain). One example is the Fourier series, which generally is used with repetitive signals, such as oscillating systems. A Fourier transform, is generally used with non-repetitive signals, such as transients. Enhanced computational techniques such as the Fast Fourier Transform (FFT) may be used for efficiency and computational speed. Yet another domain transformation is the Laplace transform, often used in electronic circuits and control systems. Yet another, the Z transform, is used with generally discrete-time signals. Digital Signal Processors (DSPs) may be advantageously utilized. Spectral density estimation may be included, along with wavelet analysis, image analysis, data compression and multivariate analysis. Correlated data sets are advantageously employed.

[0090] Difference engine may be employed to identify differences between two or more sets of data. The difference may be time based, such as where one data set relates to a time **0**, and the other set relates to a time **1**, time **2**, time **3**, . . . , time N. Differences in images may be calculated.

[0091] FIG. **11** shows a system in which the Subject response may be monitored, captured and analyzed for behavior, which is then used as input to AI. In various efforts, such as in game or entertainment design and creation, the response of the target audience may be monitored, analyzed and used to train an Artificial Intelligence or machine learning system. The subject response to entertainment/game stimuli serves to measure the ‘fun’ experienced by the subject, and that measure (the ‘fun’) is then used as a training input to AI or ML system. The system may detect individual subject behavior. Alternatively, the system may monitor group behavior, serving to detect the ‘fun’ experiences, but may also measure attributes of the group or crowd, such as ‘excitement’, ‘engagement’ or crowd based behavior.

[0092] A display is provided as a stimulus to the subject or subjects. A flat panel display or monitor may be utilized. Optionally, personal viewing devices may be utilized, such as individual screens, virtual reality headsets, augmented reality devices, heads up displays, projection devices or imaging technology.

[0093] Various detectors are utilized to monitor the one or more subject’s response. Motion detection utilizes motion tracking hardware and software. A camera images the subjects. Various cameras include the Microsoft Kinect, 2d sensors and cameras and 3d sensors and cameras. Metrics detectors may analyze the position of a body part, such as a limb, joint or facial feature. It may measure the velocity, movement, higher level derivatives of the position or movement, such as the rate of change of change. Facial detectors monitor for facial recognition. Facial attributes may be detected, such as positive attributes, e.g., a smile, or negative attributes, e.g., a frown. Body position detection may be determined. Sound detection may be performed with a microphone or microphone array. It may detect attributes of the sound, such as positive attributes, e.g., a cheer, and negative attributes, e.g., expletives, and boos. Biometric scan detection is utilized. Physiologic response detection optionally monitors the subject heart rate, blood pressure, pupil dilation, temperature, ECG, and mental activity. Activity monitoring detectors monitor engagement response, preferably including bet rate, time spent engaged with the display, retention rate, repetition rate and reengagement rate. Analytics are advantageously utilized.

[0094] The output of the system is used as input in the AI or machine learning system. For example, in training using reinforcement learning in neural networks, a positive weighting is used for positive attributes, and a negative weighting is used for negative attributes.

[0095] The system may additionally provide output identified as associated with addiction, such as gambling addiction, or a subject otherwise being ‘hooked’ on the game. When the level of engagement or minor addiction is viewed as acceptable, a positive weighting may be used in the training, whereas when the addiction is viewed as unacceptable or excessive, a negative weighting may be used in the training.

[0096] The artificial intelligence, machine learning, neural network, use of user response in training AI/ML systems (generally FIG. **11** and discussion, above), may advantageously be utilized in game design and develop, entertainment development and/or any creative developmental effort.

[0097] The systems may constitute a matrix of tools. They may comprise a given set of tools. In a more fundamental way, they comprise a tool to discover the tools. Tools may be game states, entertainment states or any form of state or matter.

[0098] The following will be described as to game development, but the tools, systems, methods and architectures may be applied to entertainment or any creative effort. As to a particular game, a first option is to provide only basic rules of that given game. The system may play against itself, or alternatively, play against other systems, in order to discovery winning game play strategies. In yet another option, the system may be provided with known gambits, with the system permitted to use or ignore the gambits. In yet an alternative embodiment, the system may be provided with a library of games. The system may analyze the library of games for game elements, game mechanics or core loops. Optionally, the system may limit analysis of the library of games to similar games, or may consider all games, optionally divided into subunits, e.g. card games, board games, video games. Once the various core loops or game elements are defined, the system may combine them in various combinations and permutations so as to define a new game or game play sequence. The system may recognize patterns in the data. Values may be assigned to decisions at various points or game states or game state decision points. The use of user response may be advantageously used in game formation and optimization. The use of user response is particularly suited to reinforced learning.

[0099] The system may operate in a hierarchical manner. Hierarchical systems may be used, where it may vary a ‘subservient’ mandated parameter so long as ‘superior’ or ‘master’ mandated parameter is met. By way of example, a ‘super’ mandated parameter’ may be used to guarantee a particular outcome. Alternatively, an administrative control may be granted, such as to set a ‘top level’ constraint.

[0100] The system may consider separate functions in a cooperative action. Functions may be reassigned or moved to other, especially lower, levels of action. The system may provide new variables. By providing a hierarchical response, core functionality may be maintained. Optionally, the system may employ a “kill switch” for the system, an apoptosis, such as based on a command such as from an administrator, or based on predefined criteria. The system may provide a package of experience ('Total Recall') such as in a continuous state and/or persistent state.

[0101] FIGS. **12** & **13** relate to various dynamic, that is changeable, systems. In the designation "d-API" and "d-SDK", 'd' stands for 'dynamic' and is capable of change within and by the system. The format of the interaction (request and/or response) may be changes. Alternately, it may change the type, quantity or quality of information provided in the response. Other factors that may be changed include the ability of the request to alter the information via the API or SDK. Changes may be made to other operational or administrative rights or permissions, such as read only access, read and write, edit rights, super administrative rights. These provide for dynamic change under adaptive control.

[0102] Within the dynamic-Application Programming Interface (d-API), an initial format for request and response is defined. This may be considered in an 'if-then' statement: IF you ask for X in an agreed upon format, THEN system will provide X. The dynamic system may vary the format, and/or response. An intelligent dynamic update may be based on AI, machine learning or analytics. While not limited to the following, some or all of these changes may be implemented dynamically: the format of the interaction (request and/or response), access to more information or functionality, e.g. read only, or modification rights, the ability to provide information or data to the system, and the ability to change data.

[0103] Within the dynamic Game Development Kit (d-GDK), an initial kit is provided. The system then permits dynamic modification of the GDK. Preferably, dynamic modification is based on AI or Machine Learning or analytics.

[0104] Dynamic Segregated Lottery (d-SL) may be provided wherein one or more functional units or the lottery may be provided. A virtualized system may be utilized, such as in the use of a virtualized server.

[0105] FIGS. **14-20** relate to a blockchain implementation for games, entertainment or other useful ends. Blockchain uses a cryptographic 'hash' to identifies each block and transaction. Each successive block contains a hash of the previous code. This permanently fixes transactions in chronological order. The blockchain utilizes both a private key and public key. The prior hash is added to the new blockchain with a nonce to form a new hash.

[0106] Cryptocurrency provides for cryptographically secure transactions. Cryptocurrency is a programmable currency or decentralized value transfer system. It is also a decentralized virtual currency or decentralized digital currency.

[0107] Proof of work, or proof of stake, is the "right" to participate in the blockchain. It must be onerous enough to prevent changes without redoing the work. Bitcoin is a created currency which is mined and serves as a reward for payment processing work. Blockchain cryptocurrency involves no transaction charges or fees paid by purchaser. There are no refund rights or chargebacks.

[0108] It may be implemented in any form of network, both public and private. Open software and proprietary software may be used. Storage may be local storage or cloud storage and computing. Analytics may be performed locally or in a cloud analytics system. Analytics As A Service (AAAS) may be performed. Systems may be permissioned v. permission less distributed systems.

[0109] FIGS. **21** through **23** relate to smart contracts. The core elements are, first, a set of promises which may be contractual or non-contractual. Second, they are specified in digital form, operate electronically, where the contractual clauses or functional outcomes embedded in code. Third, they include protocols, or technology enabled rules-based operations. Fourth, the parties perform on the promises through automated performance, in a generally irrevocable manner.

[0110] Smart contracts automate different processes and operations. In one embodiment, they automate "if-this-then-that" on self-executing basis with finality. They may provide for payments. Actions may be conditioned on a payment or payments, such as with the control of collateral based on payment.

[0111] Smart contracts may be implemented via blockchain. This forms a trusted system, which may be implemented in a business to business implementation (B to B) and/or peer-to-peer implementation. The machine-to-machine implementation permits various combinations. In one implementation, a blockchain is combined with devices comprising the Internet of Things (IoT). In yet another combination, the blockchain may be combined with devices comprising the Internet of Things in combination with artificial intelligence. Generally, the block contains smart contract program logic. It bundles together the messages relating to a particular smart contract including inputs, outputs, and logic. In yet another implementation, they may provide contracts for difference, such as in use the current market price to adjust balances and disperse cash flow.

[0112] Smart contracts are a trust shifting technology. They reduce counter-party risk. Preferably, this serves to increase credit.

[0113] Smart contracts may be implemented in various models. They may be a contract entirely in code. They may be a contract in code with separate natural language version. They may be split natural language contract with encoded performance. Alternatively, they may be a natural language contract with encoded payment mechanism.

[0114] Smart contract initiation involves a consensus. An algorithm constitutes a set of rules for how each participant in the contract processes messages. They may be implemented in a permission-less manner, wherein anyone may submit messages for processing. The submitter may be involved in consensus. Alternately, they may delegate decision making such as to an administrator or sub-group of participants. An alternative implementation is to have a permissioned system, in which the participants are limited. They are generally pre-selected. They are then subject to gated entry and be subject to the satisfaction of certain requirements and/or approval of an administrator.

[0115] Smart contracts are subject to various methods of formation. They may by agreement such as where there is a common cooperative opportunity or a defined desired outcome. These may include business practices, asset swaps, and transfer of rights. Next, conditions set for initiation of the contract. That may be by the parties themselves, or by the occurrence of some external event, such as time, other quantifiable measure or location. Typically, they generate a code, which is encrypted and chained with blockchain technology. It may be authenticated and verified. Upon execution and processing, the network updates all ledgers to indicate current state. Once verified and posted, they cannot be changed, with only additional blocks appended.

[0116] To restate, the smart contract serves as a distributed application on networks with independent built-in trust mechanisms. The program is entrusted with the unit of value combined with rules for transfer of ownership of the unit of value. They serve as self-executing programs that automatically fulfill the terms of a programmed relationship.

[0117] FIG. **20** shows a Lottery embodiment implemented as a smart contract. The method for implementing a lottery includes the following steps. A time frame is set in which to receive cryptocurrency. Second, cryptocurrency is received with owner identification within the timeframe. The window opens for a specified duration, afterwards at which the window closes. The smart contract generates or receives a random event, such as from a random number generator. The random number generator should include an algorithmic guarantee of randomness and a guarantee of no hack. The contract selects a new owner (winner) among the owner identification related cryptocurrencies. It then assigns new ownership of cryptocurrency to selected new owner (winner).

[0118] Smart contracts may be used to implement a core loop or a game mechanic. The following core loops and game mechanics comprise a partial list of those that may be implemented, including but not limited to JACKO, POKO, Hot Seat, Hi Lo, Rock, Paper Scissors, In the Zone and iLotto or other array or geography based game mechanics or core loops. Any subunit of the game mechanic or core loop may itself be used as a game mechanic or core loop.

[0119] Jacko is a game comprising the steps of: randomly selecting a target number from a first range of numbers having a minimum and maximum number, presenting an indication of the target number to the player, selecting a number for the player, the number being selected from a second range, having a minimum and maximum, where the maximum is equal to or less than of the minimum of the first range, receiving an indication from the player whether to draw again, and if so, randomly selecting a number from the second range, accumulating the total of the player's draws, and repeating this step until either the player declines to draw or the total exceeds the target number, and in the event the player declines to draw, randomly selecting numbers from the second range, accumulating those numbers, comparing them to the player's accumulated amount, and assigning as to the winner whomever has a total closest to, but not exceeding, the target.

[0120] Poko is a multi-player game where multiple indicia are awarded a predefined value, where other players have no information as to at least some of the indicia held by other players.

[0121] High Lo is a game comprising the steps of: performing a first lottery selection of a series of randomly drawn numbers, receiving from a player an indication whether the next randomly drawn number will be higher or lower than the preceding number, and if correct, awarding winnings correlated to the amount of the randomly drawn number, and continuing until the player fails to predict the high/low outcome, or elects to stop.

[0122] In the Zone is a game of chance comprising the steps of randomly selecting a player's target number within a predefined range of numbers, the range having a minimum and a maximum, randomly selecting a series of numbers for use in a lottery game, the minimum of the predefined range of numbers being at least equal to the sum of the lowest possible total for the series of the lowest possible total for the series of numbers and the maximum of the predefined range of numbers, totaling the random selected series of numbers through the conclusion of the selection, and assigning prize amounts to players having a player's number not exceeding the total based upon the proximity of the player's number and the total number.

[0123] Rock Paper Scissors is a game with three or more options having an assigned priority of options relative to one another.

[0124] Hot Seat is a game of increasing risk/reward including the ability to 'opt out' in Smart Contract. A method for game play in a multi-level game of chance culminating in a final level, comprises the steps of presenting, at a given level, a plurality of random options wherein at least one option is a positive option, another option is a negative option, and a third option requiring a further decision, receiving a selection regarding which one of the plurality of random option is selected, and if the positive option was selected, cumulating the positive option result with the prior positive option results, but if the negative option was selected, cumulating the negative option result, comparing the cumulative result with a predetermined number, and replaying the same level if the cumulative number is less than the predetermined number or terminating the game if the cumulative number equals the predetermined number, and if the third option was selected, receiving a selection regarding the decision, respecting the above steps until the player stops, the predetermined number of negative events occurring or the final level is related.

[0125] iLotto is a grid or geography based system including a display for presenting a grid of identifying objects, an input for receiving a player selection of an identifying object, a random generator for randomly selecting a winning identifying object, and a point tally system for awarding points to the player according to the rules comprising a first point value if the player selected identifying object exactly matches the winning identifying object, a second point value if the player selected identifying object is in a geometric relationship with the winning identifying object, and a third, negative, point value if the player is not awarded the first point value or the second point value.

[0126] FIG. **23** relates to implementation of mandated and variable parameters. Mandated parameters are set in smart contracts. Examples of mandated parameters include payout percentage and payout amount. Variable parameters are subject to mandated parameters, providing entertainment options.

[0127] FIG. **24** depicts a wallet serving for the electronic storage of cryptocurrency. This represents a graphical user interface ("GUI"), such as on a phone or computer display. Various forms of cryptocurrency may be displayed on the GUI and stored in the wallet. Points may be awarded, such as for loyalty, frequency and airtimes. Recent or latest transactions may be listed, indicating the date, purpose and amount. A total account value may be shown.

[0128] Cryptocurrency systems and smart contracts may be implemented in combination with other systems. One additional system comprises a frequent user or player's club system. They may be combined with other forms of 'currency lite', including micro-transactions and micro-payments. They may be used in combinations with smart properties, that is digital assets or physical things that know who their owner is. Digital assets are anything that exists in digital, typically binary, format and comes with the right to use. Examples include images, including still pictures and video or dynamic images, audible content, such as sounds, music or performances, and digital documents. Property whose ownership is controlled via distributed trusted network, e.g., blockchain using contracts. They may be further used in combination with geolocation, wherein the physical location (geolocation) of various components and architectural components are optionally a component of the system. Limits may be placed on the geography of game play. The system can ensure compliance with geolocation of data routing.

[0129] FIGS. **25** through **27** relate to systems having segregated secure functions and public functions. This provides a secure platform with multiple interfaces to public functions and public entities. The segregated secure functions provide the function of the trusted agent. The secure functions include one or more of the following. First, outcome determination. This may include the use of a random number generator (RNG) or probability engine. Second, user or player account information is stored. Third, monetary accounting or transactions are stored. Fourth, regulatory and compliance interface is performed. Fifth, interfaces such as a developer interface. Sixth, regulatory functions including Q&A testing, compliance, testing and approval may be provided.

[0130] The public functions include some or all of the following. First, the public system issues a 'call' to the secure system. A 'call' may be via an Application Programming Interface (API) or d-API. The "OPEN" system call makes calls to secure system for secure data. Second, a designer interface serves to access tools, APIs, a Development Kit (DK), and a Software Development Kit (SDK). Third, a marketplace interface serves as a lottery interface and optionally an application or app store. Fourth, an operator interface serves to interface with an operator or organizer, e.g., a charity. It preferably serves to publish, market, and sell. Fifth, the user interface permits registration, play activity and persistent history.

[0131] The system components may vary by function. Public interfaces and functions preferably comprise an "open" platform. This allows for arbitration and agreement with the secure entity regarding game operations to be performed by the secure entity, e.g., payout %, vGLEPs, who may play, and geolocation. The secure entity performs secure functions including game outcomes, financial matters and secure user data. The end users utilize a "channel mix", including but not limited to web, mobile app, mobile web, tablet, computer, display enabled Devices (wireless), touch screen equipment at retailer, e.g., countertop games. The private entity may impose rate limits and impose responsible gaming controls.

[0132] FIGS. **28** and **29** describe hybrid and hierarchical systems. A centralized system, such as a state run lottery may be combined with a decentralized system, such as a blockchain implementation. Hierarchical order may be imposed within the system. In a system using mandated and variable parameters, a hierarchy of mandated parameters may be established, and then various variable parameters may be subject to the appropriate mandated parameter. In another application, a global use rate limit may be imposed at a high level in the hierarchy. Hierarchical use rate limits may be imposed. Various topologies of systems include master slave, master over multiple slaves and circular systems.

[0133] FIG. **30** relates to a game or lottery linked credit card and credit card function. A credit card and credit functionality may be linked to lottery or other game play. Through use of the credit card, a conversion rate is established. By way of example, for every $100 of purchases, $ 1 in lottery play is made. The rate may be variable, such as based upon institution. In the event a charitable organization organized or sponsored the lottery or game, every $100 of purchases accrues $2 for the organization. A split may also be performed, such as for every $100 of purchases accrues $1 in the lottery or game for the credit card owner and $1 for the organization.

[0134] In alternative embodiments, the mobile gaming device may be connected to the gaming machine with a cable, either directly connected to a port of the gaming machine or via a network communicating with the gaming machine.

[0135] The software used to program the gaming machines and servers in accordance with the embodiments described herein may be initially stored on a ROM, such as a CD or an electronic memory device. Such CDs and devices are non-transitory computer readable mediums having the appropriate computer instructions stored thereon. The programming may also be downloaded to the gaming machines via the casino's network.

[0136] It should be appreciated that the terminals, processors, or computers described herein may be embodied in any of a number of forms, such as a rack-mounted computer, a desktop computer, a laptop computer, or a tablet computer. Additionally, a computer may be embedded in a device perhaps not generally regarded as a computer but with suitable processing capabilities, including an electronic gaming machine, a Web TV, a Personal Digital Assistant (PDA), a smart phone or any other suitable portable or fixed electronic devices.

[0137] Also, a computer may have one or more input and output devices. These devices can be used, among other things, to present a user interface. Examples of output devices that can be used to provide a user interface include printers or display screens for visual presentation of output and speakers or other sound generating devices for audible presentation of output. Examples of input devices that can be used for a user interface include keyboards, and pointing devices, such as mice, touch pads, and digitizing tablets. As another example, a computer may receive input information through speech recognition or in other audible formats.

[0138] Such computers may be interconnected by one or more networks in any suitable form, including as a local area network or a wide area network, such as an enterprise network or the Internet. Such networks may be based on any suitable technology and may operate according to any suitable protocol and may include wireless networks, wired networks or fiber optic networks. As used herein, the term "online" refers to such networked systems, including computers networked using, e.g., dedicated lines, telephone lines, cable or ISDN lines as well as wireless transmissions. Online systems include remote computers using, e.g., a local area network (LAN), a wide area network (WAN), the Internet, as well as various combinations of the foregoing. Suitable user devices may connect to a network for instance, any computing device that is capable of communicating over a network, such as a desktop, laptop or notebook computer, a mobile station or terminal, an entertainment appliance, a set-top box in communication with a display device, a wireless device such as a phone or smartphone, a game console, etc. The term "online gaming" refers to those systems and methods that make use of such a network to allow a game player to make use of and engage in gaming activity through networked, or online systems, both remote and local. For instance, "online gaming" includes gaming activity that is made available through a website on the Internet.

[0139] Also, the various methods or processes outlined herein may be coded as software that is executable on one or more processors that employ any one of a variety of operating systems or platforms. Additionally, such software may be written using any of a number of suitable programming languages and/or programming or scripting tools, and also may be compiled as executable machine language code or intermediate code that is executed on a framework or virtual machine.

[0140] In this respect, embodiments may provide a tangible, non-transitory computer readable storage medium (or multiple computer readable storage media) (e.g., a computer memory, one or more floppy discs, compact discs (CD), optical discs, digital video disks (DVD), magnetic tapes, flash memories, circuit configurations in Field Programmable Gate Arrays or other semiconductor devices, or other non-transitory, tangible computer-readable storage media) encoded with one or more programs that, when executed on one or more computers or other processors, perform methods that implement the various embodiments discussed above. The computer readable medium or media can be transportable, such that the program or programs stored thereon can be loaded onto one or more different computers or other processors to implement various aspects as discussed above. As used herein, the term "non-transitory computer-readable storage medium" encompasses only a computer-readable medium that can be considered to be an article of manufacture or a machine and excludes transitory signals.

[0141] The terms "program" or "software" are used herein in a generic sense to refer to any type of computer code or set of computer-executable instructions that can be employed to program a computer or other processor to implement various aspects of, as discussed above. Additionally, it should be appreciated that according to one aspect of this embodiment, one or more computer programs that when executed perform methods need not reside on a single computer or processor, but may be distributed in a modular fashion amongst a number of different computers or processors to implement various aspects of embodiments described herein.

[0142] Computer-executable instructions may be in many forms, such as program modules, executed by one or more computers or other devices. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Typically the functionality of the program modules may be combined or distributed as desired in various embodiments.

[0143] Also, data structures may be stored in computer-readable media in any suitable form. For simplicity of illustration, data structures may be shown to have fields that are related through location in the data structure. Such relationships may likewise be achieved by assigning storage for the fields with locations in a computer-readable medium that conveys relationship between the fields. However, any suitable mechanism may be used to establish a relationship between information in fields of a data structure, including through the use of pointers, tags, addresses or other mechanisms that establish relationship between data elements.

[0144] Various aspects of embodiments described herein may be used alone, in combination, or in a variety of arrangements not specifically discussed in the embodiments described in the foregoing and the concepts described herein are therefore not limited in their application to the details and arrangement of components set forth in the foregoing description or illustrated in the drawings. For example, aspects described in one embodiment may be combined in any manner with aspects described in other embodiments.

[0145] Also, embodiments described herein may provide a method, of which an example has been provided. The acts performed as part of the method may be ordered in any suitable way. Accordingly, embodiments may be constructed in which acts are performed in an order different than illustrated, which may include performing some acts simultaneously, even though shown as sequential acts in illustrative embodiments.

[0146] While embodiments have been described with reference to certain exemplary features thereof, those skilled in the art may make various modifications to the described embodiments. The terms and descriptions used herein are set forth by way of illustration only and not meant as limitations. In particular, although embodiments have been described by way of examples, a variety of devices would practice the inventive concepts described herein. Embodiments have been described and disclosed in various terms, the scope of the embodiments is not intended to be, nor should it be deemed to be, limited thereby and such other modifications or embodiments as may be suggested by the teachings herein are particularly reserved, especially as they fall within the breadth and scope of the claims here appended. Those skilled in the art will recognize that these and other variations are possible as defined in the following claims and their equivalents. Although the foregoing invention has been described in some detail by way of illustration and example for purposes of clarity and understanding, it may be readily apparent to those of ordinary skill in the art in light of the teachings of this invention that certain changes and modifications may be made thereto without departing from the spirit or scope of the appended claims.

[0147] All publications and patents cited in this specification are herein incorporated by reference as if each individual publication or patent were specifically and individually indicated to be incorporated by reference in their entirety.

REFERENCES

[0148] ARM, IBM, "The Internet of Things Business Index 2017, Transformation In Motion", The Economist, Intelligence Unit Limited 2017, pages 1-22.

[0149] Crosby, et al., "Blockchain Technology: Beyond Bitcoin", Applied Innovation Review, Issue No. 2, Sutardja Center for Entrepreneurship & Technology, Berkeley Engineering, June 2016, pages 1-1.9.

[0150] Fisher, "Decentralized Peer to Peer Game Assets Platform, Integration with Third Party Games using Smart Contract," Aug. 4, 2014, 12 pages.

[0151] Hinton et al., "A Fast Learning Algorithm For Deep Belief Nets", Neural Computation, 18, 1527-1554, 2006.

[0152] Jouppi, et al., "In-Datacenter Performance Analysis of a Tensor Processing Unit™", To appear at the 44th International Symposium on Computer Architecture (ISCA), Toronto, Canada, Jun. 26, 2017, pages 1-17.

[0153] LeCun, et al., "Deep Learning", Nature, Vol. 521, 28 May 2015, pages 436-444.

[0154] Marvin, "Blockchain A-Z: Everything You Need to Know About the Game-Changing Tech Beneath Bitcoin", Jun. 3, 2016, 9 pages.

[0155] Marvin, "Blockchain: The Invisible Technology That's Changing the World", Feb. 6, 2017, 32 pages.

[0156] Mougayar, The Business Blockchain, pages 6-9, 128-133, 2016, published by John Wiley & Sons, Hoboken, N.J.

[0157] Nakamoto, "Bitcoin—A Peer to Peer Electronic Cash System", 2008, pages. 1-9 Ng, "What Artificial Intelligence Can and Can't Do Right Now", Harvard Business Review, Nov. 9, 2016, 5 pages.

[0158] O'Dowd, et al., "IBM's Open Blockchain, Making Blockchain Real for Enterprises", IBM Blockchain, April 2016, pages 1-20.

[0159] Ronan, "Deep Learning predicts Loto Numbers", Academy of Paris, Apr. 1, 2016, pages 1-4.

[0160] Smart Contract Alliance, "Smart Contracts: 12 Use Cases for Business and Beyond, A Technology, Legal & Regulatory Information, prepared by Smart Contracts Alliance—In collaboration with Deloitte, An industry initiative of the Chamber of Digital Commerce". December 2016, pages 1-53.

[0161] Turing, "Computing Machinery and Intelligence", Mind 49: 1950, pages 433-460.

[0162] Wood, "Ethereum: A Secure Decentralized Generalized Transaction Ledger", Homestead Draft, 2014, pages 1-32.

[0163] Wu, et al., "Google's Neural Machine Translation System: Bridging the Gap between Human and Machine Translation", 8 Oct. 2016, pages 1-23.

[0164] Yli-Huumo, et al., "Where Is Current Research on Blockchain Technology? A Systematic Review", Oct. 3, 2016, pages 1-27.

Glossary

[0165] 51% Attack: An attack on the Bitcoin network which allows the attacker to create fraudulent transactions, see Double Spend. This is possible because controlling more than 50% of the Bitcoin network's hash rate means the attacker can out-compute everyone else who is mining.

A

[0166] Account: Accounts have an intrinsic balance and transaction count maintained as part of the Ethereum state. They also have some (possibly empty) EVM Code and a (possibly empty) Storage State associated with them. Though homogenous, it makes sense to distinguish between two practical types of account: those with empty associated EVM Code (thus the account balance is controlled, if at all, by some external entity) and those with non-empty associated EVM Code (thus the account represents an Autonomous Object). Each Account has a single Address that identifies it.

[0167] Address: A bitcoin address is used to receive and send transactions on the bitcoin network. It contains a string of alphanumeric characters, but can also be represented as a scannable QR code. A bitcoin address is also the public key in the pair of keys used by bitcoin holders to digitally sign transactions (see Public Key).

[0168] Address: A code, e.g. a 160-bit code, used for identifying Accounts.

[0169] Agreement Ledger: An agreement ledger is distributed ledger used by two or more parties to negotiate and reach agreement.

[0170] Airdrop: A method of distributing cryptocurrency amongst a population, first attempted with Auroracoin (auroracoin) in early 2014.

[0171] Algorithm: A process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer.

[0172] Altcoin: The collective name for cryptocurrencies offered as alternatives to bitcoin. Litecoin, Feathercoin and PPcoin are all altcoins.

[0173] AML: Anti-Money Laundering techniques are used to stop people converting illegally obtained funds, to appear as though they have been earned legally. AML mechanisms can be legal or technical in nature. Regulators frequently apply AML techniques to bitcoin exchanges.

[0174] App: An end-user-visible application, e.g. hosted in the Ethereum Browser.

[0175] Application Program Interface (API): A specification used as an interface by components, often software components, to communicate with one another. May include specifications for routines, data structures, object classes, and variables.

[0176] Arbitrage: The generation of risk free profits by trading between markets which have different prices for the same asset.

[0177] ASIC: An Application Specific Integrated Circuit is a silicon chip specifically designed to do a single task. In the case of bitcoin, they are designed to process SHA-256 hashing problems to mine new bitcoins.

[0178] ASIC Miner: A piece of equipment containing an ASIC chip, configured to mine for bitcoins. They can come in the form of boards that plug into a backplane, devices with a USB connector, or standalone devices including all of the necessary software, that connect to a network via a wireless link or ethernet cable.

[0179] ASIC Mining: Many miners purchase separate computing devices set aside solely for mining. As an alternative, they can also get an Application Specific Integrated Circuit (ASIC); this is a specially-designed computer chip created to perform one specific function, and only that function—in this case, mining calculations. ASICs reduce the processing power and energy required for mining, and can help reduce the overall cost of the process in that way. Whether the ASIC—a term that refers to the specialized chip itself—is integrated into an existing computing system, or functions as a stand-alone device, the term "ASIC" is often used generically to refer to the overall system itself, and not just the chip.

[0180] Asymmetric Key Algorithm: This is the algorithm used to generate public and private keys, the unique codes that are essential to cryptocurrency transactions. In a symmetric key algorithm, both the sender and receiver have the same key; they can encrypt and exchange information privately, but since both parties have the decoding information, they can't keep information private from one another. With an asymmetric key algorithm, both parties have access to the public key, but only the person with the private key can decode the encryption; this assures that only they can receive the funds.

[0181] Attestation Ledger: A distributed ledger providing a durable record of agreements, commitments or statements, providing evidence (attestation) that these agreements, commitments or statements were made.

[0182] Autonomous Agents: Software that makes decisions and acts on them without human intervention.

[0183] Autonomous Object: A notional object existent only within the hypothetical state of Ethereum. Has an intrinsic address and thus an associated account; the account will have non-empty associated EVM Code. Incorporated only as the Storage State of that account.

B

[0184] Base58: Base58 encodes binary data into text and is used to encode Bitcoin addresses. Created by Satoshi Nakamoto, its alphanumeric characters exclude "0", "O", "1", I" since they are hard to distinguish.

[0185] Base58Check: A variant of Base58 used to detect typing errors in bitcoin addresses.

[0186] BIP: An acronym for "Bitcoin Improvement Proposals" which can be submitted by anyone who wants to improve the Bitcoin network.

[0187] Bit: Name of a Bitcoin denomination equal to 100 satoshis (1 millionth of 1 BTC). In 2014 several companies including Bitpay and Coinbase, and various wallet apps adopted bit to display bitcoin amounts.

[0188] Bitcoin (uppercase): The well know cryptocurrency, based on the proof-of-work blockchain.

[0189] bitcoin (lowercase): The specific collection of technologies used by Bitcoin's ledger, a particular solution. Note that the currency is itself one of these technologies, as it provides the miners with the incentive to mine.

[0190] Bitcoin (unit of currency): 100,000,000 satoshis. A unit of the decentralized, digital currency which can be traded for goods and services. Bitcoin also functions as a reserve currency for the altcoin ecosystem.

[0191] Bitcoin 2.0: A reference word for applications of bitcoin or Blockchain technology that is more advanced or complicated than the basic payment system application proposed by the Bitcoin white paper. Examples of Bitcoin 2.0 projects include Counterparty, Ethereum, Blockstream, Swarm, Domus and Hedgy.

[0192] Bitcoin ATM: A bitcoin ATM is a physical machine that allows a customer to buy bitcoin with cash. There are many manufacturers, some of which enable users to sell bitcoin for cash. They are also sometimes called 'BTMs' or 'Bitcoin AVMS'. CoinDesk maintains a worldwide map of operational bitcoin ATM machines and a list of manufacturers.

[0193] Bitcoin Core: New name of Bitcoin QT since release of version 0.9 on Mar. 19, 2014. Not to confuse with CoreBitcoin, an Objective-C implementation published in August 2013.

[0194] Bitcoind: Original implementation of Bitcoin with a command line interface. Currently a part of BitcoinQT project. "D" stands for "daemon" per UNIX tradition to name processes running in background.

[0195] Bitcoin Days Destroyed: An estimate for the "velocity of money" with the Bitcoin network. This is used because it gives greater weight to bitcoins that have not been spent for a long time, and better represents the level of economic activity taking place with bitcoin than total transaction volume per day.

[0196] Bitcoin Investment Trust: This private, open-ended trust invests exclusively in bitcoins and uses a state-of-the-art protocol to store them safely on behalf of its shareholders. It provides a way for people to invest in bitcoin without having to purchase and safely store the digital currency themselves.

[0197] Bitcoinj: A Java implementation of a full Bitcoin node by Mike Hearn. Also includes SPV implementation among other features.

[0198] BitcoinJS: An online library of javascript code used for Bitcoin development, particularly web wallets. bitcoinjs.org (http://bitcoinjs.org)

[0199] Bitcoin Market Potential Index (BMPI): The Bitcoin Market Potential Index (BMPI) uses a data set to rank the potential utility of bitcoin across **177** countries. It attempts to show which markets have the greatest potential for bitcoin adoption.

[0200] Bitcoin Network: The decentralized, peer-to-peer network which maintains the blockchain. This is what processes all Bitcoin transactions.

[0201] Bitcoin Price Index (BPI): The CoinDesk Bitcoin Price Index represents an average of bitcoin prices across leading global exchanges that meet criteria specified by the BPI. There is also an API for developers to use.

[0202] Bitcoin Protocol: The open source, cryptographic protocol which operates on the Bitcoin network, setting the "rules" for how the network runs.

[0203] BitcoinQT: Bitcoin QT is an open source software client used by your computer. It contains a copy of the blockchain and once installed it turns your computer into a node in the Bitcoin Network. Also acts as a "desktop wallet."

[0204] Bitcoin-ruby: A Bitcoin utilities library in Ruby by Julian Langschaedel. Used in production on Coinbase.com

[0205] Bitcoin Sentiment Index (BSI): The Bitcoin Sentiment Index is a measure of whether individuals feel the digital currency's prospects are increasing or decreasing on any given day, and is powered by data collected by Qriously.

[0206] Bitcoin Whitepaper: The bitcoin whitepaper was written by 'Satoshi Nakamoto' and posted to a Cryptography Mailing list in 2008. The paper describes the bitcoin protocol in detail, Satoshi Nakamoto followed this by releasing the bitcoin code in 2009.

[0207] Bitcoin white paper: In November 2008, a paper, authored (probably pseudonymously) by Satoshi Nakamoto, was posted on the newly created Bitcoin.org website with the title 'Bitcoin: A Peer-to-Peer Electronic Cash System'. The eight-page document described methods of using a peer-to-peer network to generate "a system for electronic transactions without relying on trust" and laid down the working principles of the cryptocurrency.

[0208] Bitcore: A Bitcoin toolkit by Bitpay written in JavaScript. More complete than Bitcoinjs.

[0209] BitPay: A payment processor for bitcoins, which works with merchants, enabling them to take bitcoins as payment.

[0210] BitStamp: An exchange for bitcoins that has been gaining in popularity.

[0211] Block: This is a collection of transaction data, one of the fundamental elements of cryptocurrency. As transactions are made, the pertinent information for each one is collected, and when the gathered data reaches a predetermined size, it's bundled up as a block. As soon as possible after blocks are created, they're processed by investors for transaction verification; this process is known as mining.

[0212] Blockchain: The full list of blocks that have been mined since the beginning of the bitcoin cryptocurrency. The blockchain is designed so that each block contains a hash drawing on the blocks that came before it. This is designed to make it more tamperproof. To add further confusion, there is a company called Blockchain, which has a very popular blockchain explorer and bitcoin wallet.

[0213] Block Halving: [see Halving] The halving of the bitcoin reward that miners receive for mining a block. This takes place approximately every 4 years (every 210,000 block to be precise).

[0214] Block Header: Contains information about a block, such as the hash of the previous block header, its version number, the current target, a timestamp, and a nonce.

[0215] Block Height: Block height refers to the number of blocks connected together in the block chain. For example, Height 0, would be the very first block, which is also called the Genesis Block.

[0216] Blockchain.info: A web service running a Bitcoin node and displaying statistics and raw data of all the transactions and blocks. It also provides a web wallet functionality with lightweight clients for Android, iOS and OS X.

[0217] Block Reward: The reward given to a miner which has successfully hashed a transaction block. This can be a mixture of coins and transaction fees, depending on the policy used by the cryptocurrency in question, and whether all of the coins have already been successfully mined. Bitcoin currently awards 25 bitcoins for each block. The block reward halves when a certain number of blocks have been mined. In bitcoin's case, the threshold is every 210,000 blocks.

[0218] Bootstrapping: Technique for uploading the program onto a volunteer's computer or mobile device through a few simple instructions that set the rest of the program in motion.

[0219] BOT Trading: Software programs that operate on trading platforms, executing buy and sell orders with preprogrammed trading instructions.

[0220] Brain Wallet: [see Wallet] A bitcoin wallet which uses a long string of words to secure its coins. This "passphrase" can be memorized, allowing the wallet owner to spend bitcoins by simply remembering the passphrase.

[0221] Brainwallet.org: Utility based on bitcoin to craft transactions by hand, convert private keys to addresses and work with a brain wallet.

[0222] BTC: The short currency abbreviation for bitcoins.

[0223] Buy Order: A buy order is established when an investor approaches an exchange and wants to purchase cryptocurrency. These can range from very simple orders ("I want to spend x amount of dollars on Bitcoins") to complex ones that include factors such as time frame in which the order should be filled, range of price, and so forth. Most exchanges allow for these to be entered online, but some investors prefer to go over the details directly with an exchange representative. Buy orders don't necessarily guarantee your purchase; if your price is too low, for example, the offer may expire without being filled unless you make adjustments

C

[0224] Capital Controls: These are local measures such as transaction taxes, limits, or other prohibitions that a government can use to regulate flows from capital markets into and out of the country.

[0225] Casascius Coins: Physical collectible coins produced by Mike Caldwell. Each coin contains a private key under a tamper-evident hologram. The name "Casascius" is formed from a phrase "call a spade a spade", as a response to a name of Bitcoin itself.

[0226] Central Ledger: A central ledger refers to a ledger maintained by a central agency.

[0227] Change: Informal name for a portion of a transaction output that is returned to a sender as a "change" after spending that output. Since transaction outputs cannot be partially spent, one can spend 1 BTC out of 3 BTC output only be creating two new outputs: a "payment" output with 1 BTC sent to a payee address, and a "change" output with remaining 2 BTC (minus transaction fees) sent to the payer's addresses. BitcoinQT always uses new address from a key pool for a better privacy. Blockchain.info sends to a default address in the wallet. A common mistake when working with a paper wallet or a brain wallet is to make a change transaction to a different address and then accidentally delete it. E.g. when importing a private key in a temporary Bitcoin QT wallet, making a transaction and then deleting the temporary wallet.

[0228] Checkpoint: A hash of a block before which the BitcoinQT client downloads blocks without verifying digital signatures for performance reasons. A checkpoint usually refers to a very deep block (at least several days old) when it is clear to everyone that the block is accepted by the overwhelming majority of users and reorganization with not happen past that point. It also helps protecting most of the history from a 51% attack. Since checkpoints affect how the main chain is determined, they are part of the protocol and must be recognized by alternative clients (although the risk of reorganization past the checkpoint would be incredibly low).

[0229] Circle: Circle is an exchange and wallet service, offering users worldwide the chance to store, send, receive and exchange bitcoins.

[0230] Client: A software program running on a desktop or laptop computer, or mobile device. It connects to the bitcoin network and forwards transactions. It may also include a bitcoin wallet (see Node).

[0231] the Cloud: A reference to the Internet and functions it can carry out for anyone such as storage, file sending, and using apps.

[0232] Cloud-hashing/mining: A type of mining where people can pay to rent computer power from someone else in the cloud to mine bitcoin or other cryptocurrencies. This is done by selling mining contracts. Cloudhashing is also the name of a business which offers this service.

[0233] Coin: An informal term that means either 1 bitcoin, or an unspent transaction output that can be spent.

[0234] Coin Age: The age of a coin, defined as the currency amount multiplied by the holding period.

[0235] Coinbase: Another name for the input used in a bitcoin's generation transaction. When a bitcoin is mined, it doesn't come from another bitcoin user, but is generated as a reward for the miner. That reward is recorded as a transaction, but instead of another user's bitcoin address, some arbitrary data is used as the input. Coinbase is also the name of a bitcoin wallet service that also offers payment processing services for merchants and acts as an intermediary for purchasing bitcoins from exchanges.

[0236] Coinbase.com: US-based Bitcoin/USD exchange and web wallet service.

[0237] Cold Storage: The safest way to store private keys is by keeping them offline in “cold storage”. This could be in the form of a hardware wallet, USB stick or paper wallet. These wallets are known as “cold wallets”.

[0238] Collective Mining: The commitment of resources and materials to the process of mining digital currency data blocks often proves to be too expensive for individuals to take part. As a result, many enterprising businesses have worked out a way to make mining more affordable for those miners who would otherwise be left out. These companies invest in the hardware that allows for high-end mining power, and they in turn lease the access to this mining capability to third parties. As an individual miner, this means you can sign a contract that allows you to use a predetermined amount of mining power through cloud computing, without the hassle or expense of buying or maintaining the processing power needed to do so. The block rewards that come with the successful mining of the data block go to the individual miner who purchased the contract from the collective mining company.

[0239] Colored Coins: A proposed add-on function for bitcoin that would enable bitcoin users to give them additional attributes. These attributes could be user-defined, enabling you to mark a bitcoin as a share of stock, or a physical asset. This would enable bitcoins to be traded as tokens for other property.

[0240] CompactSize: Original name of a variable-length integer format used in transaction and block serialization. Also known as “Satoshi’s encoding”. It uses 1, 3, 5 or 9 bytes to represent any 64-bit unsigned integer. Values lower than 253 are represented with 1 byte. bytes 253, 254 and 255 indicate 16-, 32- or 64-bit integer that follows. Smaller numbers can be presented different. In bitcoin-ruby it is called “var_int”, in Bitcoinj it is Varint. BitcoinQT also has even more compact representation called Varint which is not compatible with CompactSize and used in block storage.

[0241] Confirmation: The act of hashing a bitcoin transaction successfully into a transaction block, and cementing its validity. A single confirmation will take around 10 minutes, which is the average length of time for a transaction block to be hashed. However, some more sensitive or larger transactions may require multiple confirmations, meaning that more blocks must be hashed and added to the blockchain after the transaction’s block has been hashed. Each time another block is added to the blockchain after the transaction’s block, the transaction is confirmed again.

[0242] Confirmation Number: Confirmation number is a measure of probability that transaction could be rejected from the main chain. “Zero confirmations” means that transaction is unconfirmed (not in any block yet). One confirmation means that the transaction is included in the latest block in the main chain. Two confirmations means the transaction is included in the block right before the latest one. Probability of transaction being reversed (“double spent”) is diminishing exponentially with more blocks added “on top” of it.

[0243] Confirmed Transaction: Transaction that has been included in the blockchain. Probability of transaction being rejected is measured in a number of confirmations.

[0244] Consensus Point: A point—either in time, or defined in terms of a set number or volume of records to be added to the ledger—where peers meet to agree the state of the ledger.

[0245] Consensus Process: The process a group of peers responsible for maintaining a distributed ledger used to reach consensus on the ledger’s contents.

[0246] Contract: Informal term used to mean both a piece of EVM Code that may be associated with an Account or an Autonomous Object.

[0247] Core Developers: Programmers working on the open-source Source Code for Bitcoin. They are not formally employed by or paid by, and are not in control of, the Bitcoin Network; however, they have elevated access on the GitHub resource page for the Bitcoin Network where the main “reference” version of the Source Code is developed.

[0248] Counterfeiting: The act of imitating something in order to commit fraudulent behavior. An example of this is shopping with fake money.

[0249] CPU: Central Processing Unit—the ‘brain’ of a computer. In the early days, these were used to hash bitcoin transactions, but are now no longer powerful enough. They are still sometimes used to hash transactions for altcoins.

[0250] Crowdsourcing: The pooling of resources such as information or money contributed by the general population, to a goal. This is usually done online via websites where people can donate.

[0251] Cryptocurrency: A form of currency based on mathematics alone. Instead of fiat currency, which is printed, cryptocurrency is produced by solving mathematical problems based on cryptography.

[0252] Cryptography: The use of mathematics to create codes and ciphers that can be used to conceal information. Used as the basis for the mathematical problems used to verify and secure bitcoin transactions.

[0253] CSRNG: Acronym for “Cryptographically Secure Random Number Generator”, used in private key generation for bitcoin wallets.

[0254] Cyberclones: Created by corporations by fracking digital world for their data.

D

[0255] DAO: An acronym for “Decentralised Autonomous Organization”, a theoretical company that could exist in the cloud and carry out business according to preset algorithms, needing no human management. Also known as “DACs”.

[0256] Darksend: Darksend is Darkcoin’s decentralized mixing implementation, which was designed to give users of Darkcoin greater transactional privacy/anonymity.

[0257] DDoS: A distributed denial of service attack uses large numbers of computers under an attacker’s control to drain the resources of a central target. They often send small amounts of network traffic across the Internet to tie up computing and bandwidth resources at the target, which prevents it from providing services to legitimate users. Bitcoin exchanges have sometimes been hit with DDoS attacks.

[0258] Deepweb: The content online not indexed by search engines making it difficult to access. The majority of content on the Internet resides on the deepweb and can be accessed using a program called TOR.

[0259] Demurrage: Certain currencies penalize users for hoarding, this is done via demurrage, where a fee is charged for holding unspent coins. This fee increases as time passes.

[0260] Denial of Service [DoS]: Is a form of attack on the network. Bitcoin nodes punish certain behavior of other nodes by banning their IP addresses for 24 hours to avoid DoS. Also, some theoretical attacks like 51% attack may be used for network-wide DoS.

[0261] Depth: Depth refers to a place in the blockchain. A transaction with 6 confirmations can also be called "6 blocks deep".

[0262] Desktop Wallet: A wallet that stores the private keys on your computer, which allow the spending and management of your bitcoins.

[0263] Deterministic Wallet: A wallet based on a system of deriving multiple keys from a single starting point known as a seed. This seed is all that is needed to restore a wallet if it is lost and can allow the creation of public addresses without the knowledge of the private key.

[0264] Difficulty: This number determines how difficult it is to hash a new block. It is related to the maximum allowed number in a given numerical portion of a transaction block's hash. The lower the number, the more difficult it is to produce a hash value that fits it. Difficulty varies based on the amount of computing power used by miners on the bitcoin network. If large numbers of miners leave a network, the difficulty would decrease.

[0265] Digital Certificate: Pieces of code that protect messages without the encrypt-decrypt operations but users must apply (and pay an annual fee) for individual certificates and most common e-mail services do not support them (Google, Outlook, Yahoo).

[0266] Digital Commodity: A digital commodity is a scarce, electronically transferable, intangible, with a market value.

[0267] Digital Identity: A digital identity is an online or networked identity adopted or claimed in cyberspace by an individual, organization or electronic device.

[0268] Distributed Autonomous Enterprise [DAE]: Requires little or no traditional management or hierarchy to generate customer value and owner wealth.

[0269] Distributed Application [DAPP]: A set of smart contracts that stores data on a home-listings blockchain.

[0270] Distributed Capitalism: Lowering barriers to participation.

[0271] Distributed Ledger: Distributed ledgers are a type of database that are spread across multiple sites, countries or institutions. Records are stored one after the other in a continuous ledger. Distributed ledger data can be either "permissioned" or "unpermissioned" to control who can view it.

[0272] Double Spending: The act of spending bitcoins twice. It happens when someone makes a transaction using bitcoins, and then makes a second purchase from someone else, using the same bitcoins. They then convince the rest of the network to confirm only one of the transactions by hashing it in a block. Double spending is not easy to do, thanks to the way that the bitcoin network operates, but it is nevertheless a risk run by those accepting zero-confirmation transactions.

[0273] Dust: A transaction output that is smaller than a typically fee required to spend it [sic]. This is not a strict part of the protocol, as any amount more than zero is valid. BitcoinQT refuses to mine or relay "dust" transactions to avoid uselessly increasing the size of unspent transaction outputs (UTXO) index.

[0274] Dust Transaction: A transaction for an extremely small amount of bitcoins, which offers little financial value, but takes up space in the blockchain. The bitcoin developer team has taken efforts to eliminate dust transactions by increasing the minimum transaction amount that will be relayed by the network.

E

[0275] ECDSA: The Elliptic Curve Digital Signature Algorithm is the lightweight cryptographic algorithm used to sign transactions in the Bitcoin protocol.

[0276] Elliptic Curve Arithmetic: A set of mathematical operations defined on a group of points on a 2D elliptic curve. Bitcoin protocol uses predefined curve secp256k1. Here is the simplest possible explanation of the operations: you can add and subtract points and multiply them by an integer. Dividing by an integer is computationally infeasible (otherwise cryptographic signatures will not work). The private is a 256-bit integer and the public key is a product of a predefined point G ("generator") by that integer: A=G*a. Associativity law allows implementing interesting cryptographic schemes like Diffie-Hellman key exchange (ECDH): two parties with private keys a and b may exchange their public keys A and B to compute a shared secret point C:C+A*b=B*a because (G*a)*==(G*b)*a. The this point C can be used as a AES encryption key to protect their communication channel.

[0277] 'Entertainment': states, displays, user experience, stimuli (light, sound, tactile), Title/Value Transfer, game

[0278] Escrow: The act of holding funds or assets in a third-party account to protect them during an asynchronous transaction.

[0279] ETF: Acronym for "Exchange Traded Fund". These are investment funds traded on stock markets that track the price index of an underlying asset.

[0280] Ethereum Browser: (aka Ethereum Reference Client) A cross-platform GUI of an interface similar to a simplified browser (a la Chrome) that is able to host sandboxed applications whose backend is purely on the Ethereum protocol.

[0281] Ethereum Runtime Environment: (aka ERE) The environment which is provided to an Autonomous Object executing in the EVM. Includes the EVM but also the structure of the world state on which the EVM relies for certain I/O instructions including CALL & CREATE.

[0282] Ethereum Virtual Machine: (aka EVM) The virtual machine that forms the key part of the execution model for an Account's associated EVM Code.

[0283] EVM Assembly: The human-readable form of EVM code.

[0284] EVM Code: The bytecode that the EVM can natively execute. Used to formally specify the meaning and ramifications of a message to an Account.

[0285] Exchange: A central resource for exchanging different forms of money and other assets. Bitcoin exchanges are typically used to exchange the cryptocurrency for other, typically fiat, currencies.

[0286] External Actor: A person or other entity able to interface to an Ethereum node, but external to the world of Ethereum. It can interact with Ethereum through depositing signed Transactions and inspecting the blockchain and associated state. Has one (or more) intrinsic Accounts.

[0287] Extra Nonce: A number placed in coinbase script and incremented by a miner each time the nonce 32-bit integer overflows. This is not the required way to continue mining when nonce overflows, one can also change the merkle tree of transactions or change a public key used for collecting a block reward.

F

[0288] Faucet: A technique used when first launching an altcoin. A set number of coins are pre-mined, and given away for free, to encourage people to take interest in the coin and begin mining it themselves.

[0289] Fiat Currency: A currency, conjured out of thin air, which only has value because people say it does. Constantly under close scrutiny by regulators due to its known application in money laundering and terrorist activities. Not to be confused with bitcoin.

[0290] Fill or Kill: This is a simple type of buy order made with a cryptocurrency exchange. The investor dictates how much currency they want, and at what price, and establishes a cutoff date for the order. The exchange will then do their best to fill the order according to those criteria. If the exchange hasn't found an appropriate match for the order by the cutoff date, the order is canceled and left unfilled. In other words, fill this order according to these guidelines and within this time frame. If you can't, kill it

[0291] FinCEN: The Financial Crimes Enforcement Network, an agency within the US Treasury Department. FinCEN has thus far been the main organization to impose regulations on exchanges trading in bitcoin.

[0292] Fork: The creation of an alternative ongoing version of the blockchain, typically because one set of miners begins hashing a different set of transaction blocks from another. It can be caused maliciously, by a group of miners gaining too much control over the network (see 51% attack), accidentally, thanks to a bug in the system, or intentionally, when a core development team decides to introduce substantial new features into a new version of a client. A fork is successful if it becomes the longest version of the blockchain, as defined by difficulty.

[0293] FPGA: A Field Programmable Gate Array is a processing chip that can be configured with custom functions after it has been fabricated. Think of it as a blank silicon slate on which instructions can be written. Because FPGAs can be produced en masse and configured after fabrication, manufacturers benefit from economies of scale, making them cheaper than ASIC chips.

[0294] Freicoin: A cryptocurrency based on the inflation-free principles outlined by the economist Silvio Gessell.

[0295] Frictionless: In reference to payment systems, a system is "frictionless" when there are zero transaction costs or restraints on trading.

[0296] Full Node: A node which implements all of bitcoin protocol and does not require trusting any external service to validate transactions. It is able to download and validate the entire blockchain. All full nodes implement the same peer-to-peer messaging protocol to exchange transactions and blocks, but that is not a requirement. A full node may receive and validate data using any protocol and from any source. However, the highest security is achieved by being able to communicate as fast as possible with as many nodes as possible.

G

[0297] Gas: The fundamental network cost unit. Paid for exclusively by Ether (as of PoC-4), which is converted freely to and from Gas as required. Gas does not exist outside of the internal Ethereum computation engine; its price is set by the Transaction and miners are free to ignore Transactions whose Gas price is too low.

[0298] Genesis Block The very first block in the block chain.

[0299] Gigahashes/sec: The number of hashing attempts possible in a given second, measured in billions of hashes (thousands of Megahashes).

[0300] GPU: Graphical Processing Unit. A silicon chip specifically designed for the complex mathematical calculations needed to render millions of polygons in modern computer game graphics. They are also well suited to the cryptographic calculations needed in cryptocurrency mining.

[0301] Graph Gaps: On occasion, gaps will appear in trend lines on market value graphs. These gaps indicate a visible drop or rise in a commodity's value that hasn't necessarily happened due to trading. These can be the result of closed markets, statistical adjustments by analysts, or by strong news about the commodity. There are three types of gaps:

[0302] 1. Breakaway Gap. These appear at the beginning of a strong upward or downward trend, and represent very high-volume trading.

[0303] 2. Runaway Gap. These occur during an upward or downward trend, and represent a quick momentary intensification of that trend.

[0304] 3. Exhaustion Gap. This occurs toward the end of an upward or downward trend, and tends to indicate a small trend in the opposite direction

H

[0305] Halving: Bitcoins have a finite supply, which makes them a scarce digital commodity. The total amount of bitcoins that will ever be issued is 21 million. The number of bitcoins generated per block is decreased 50% every four years. The final halving will take place in the year 2140.

[0306] Hard Fork: Some people use term hard fork to stress that changing Bitcoin protocol requires overwhelming majority to agree with it, or some noticeable part of the economy will continue with original blockchain following the old rules.

[0307] Hardware Wallet: A bitcoin wallet which stores users bitcoins offline on hardware devices

[0308] Hash: A mathematical process that takes a variable amount of data and produces a shorter, fixed-length output. A hashing function has two important characteristics. Firstly, it is mathematically difficult to work out what the original input was by looking at the output. Secondly, changing even the tiniest part of the input will produce an entirely different output.

[0309] to HASH: To compute a hash function of some data. If hash function is not mentioned explicitly, it is the one defined by the context. For instance, "to hash a transaction" means to compute Hash256 of binary representation of a transaction.

[0310] Hash160: SHA-256 hashed with RIPEMD-160 it is used to produce an address because it makes a smaller hash (20 bytes vs. 32 bytes) than SHA-256, but still uses SHA-

256 internally for security. BTCHash160( ) in CoreBitcoin. Hash160( ) in BitcoinQT. It is also available in scripts as OP_HASH160.

[0311] Hash, Hash256: When not speaking about arbitrary hash functions, Hash refers to two rounds of SHA-256. That is, you should compute a SHA-256 hash of your data and then another SHA-256 hash of that hash. It is used in block header hashing, transaction hashing, making a merkle tree of transactions, or computing a checksum of an address. Known as BTCHash2560( ) in CoreBitcoin, Hash( ) in BitcoinQT. It is also available in scripts as OP_HASH256.

[0312] Hash Function: A hash function takes an arbitrary input such as a string of integers (a key) and outputs a value of a pre-specified length (a hash). Bitcoin uses a cryptographic hash function to secure the network.

[0313] Hash Rate: The number of hashes that can be performed by a bitcoin miner in a given period of time (usually a second).

[0314] Hash Type (hashtype): A single byte appended to a transaction signature in the transaction input which describes how the transaction should be hashed in order to verify that signature. There are three types affecting outputs: ALL (default), SINGLE, NONE and one optional modifier ANYONECANPAY affecting the inputs (can be combined with either of the first three). ALL requires all outputs to be hashed (thus, all outputs are signed). SINGLE clears all output scripts but the one with the same index as the input in question. NONE clears all outputs thus allowing changing them at will. ANYONECANPAY removes all inputs except the current one (allows anyone to contribute independently.) The actual behavior is more subtle than this overview, you should check the actual source code for more comments.

[0315] Height: See Block Height

[0316] Hot Wallet: A bitcoin wallet that has an active connection to the Internet. These are used for "everyday" transactions and should never hold large amounts of bitcoin, since their connectivity reduces their security.

[0317] HTML: Acronym for "HyperText Markup Language", the language in which webpages are written.

[0318] HTTP: Acronym for "HyperText Transfer Protocol", this is the underlying protocol for the world wide web.

[0319] Hybrid Wallet: This is a cryptocurrency storage and maintenance system that is a combination of a software wallet (stored on a local computer) and a web wallet (stored on a third-party server). The bulk of your digital currency account information is stored on the wallet host's server—except for one important detail. Your private key (the code that uniquely identifies you) is stored only on your own device. When you make a transaction, your private key is encrypted on the way to the exchange's server, so they never know what your private key is. Access to your private key also includes a password that again only the user knows. If the user loses or forgets that password, access to the account could be denied, and the user could potentially lose the account balance forever.

I

[0320] Industrial Blockchain: Secure transactional capability to watches and other wearable devices.

[0321] Input: The part of a bitcoin transaction denoting where the bitcoin payment has come from. Typically, this will be a bitcoin address, unless the transaction is a generation transaction, meaning that the bitcoin has been freshly mined (see Coinbase).

[0322] Interface System and methods by which two or more computers talk to each other over a network, such as the Internet, using a common language that they both understand.

K

[0323] Key: Could mean an ECDSA public or private key, or AES symmetric encryption key. AES is not used in the protocol itself (only to encrypt the ECDSA keys and other sensitive data), so usually the word key means an ECDSA key. When talking about keys, people usually mean private keys as public key can always be derived from a private one. See Private Key and Public Key.

[0324] Key Pool: Some wallet applications that create new private keys randomly keep a pool of unused pre-generated keys (BitcoinQT keeps 100 keys by default). When a new key is needed for change address or a new payment request, the application provides the oldest key from the pool and replaces it with a fresh one. The purpose of the pool is to ensure that recently used keys are always already back up on external storage. Without a key pool you could create a new key, receive a payment on its address and then have your hard disk died before backing up this key. A key pool guarantees that this key was already backed up several days before being used. Deterministic wallets do not use a key pool because they need to back up a single secret key.

[0325] Kilohashes/sec: The number of hashing attempts possible in a given second, measured in thousands of hashes.

[0326] Kimoto Gravity Well: A mining difficult readjustment algorithm, which was created in 2013 for Megacoin, an altcoin. The well allows difficulty readjustment to occur every block, instead of every 2016 blocks for Bitcoin. This was done as a response to concern about multi pool mining schemes.

[0327] KYC: Know Your Client/Customer rules force financial institutions to vet the people they are doing business with, ensuring that they are legitimate.

L

[0328] Laundry: Also known as a "mixing service", they combine funds from various users and redistribute them, making tracing the bitcoins back to their original source very difficult by mixing their "taint".

[0329] Ledger: An append-only record store, where records are immutable and may hold more general information than financial records.

[0330] Ledger of Everything: Blockchain can address the six obstacles to a functioning Internet of Things features: resilient, robust, real-time, responsive, radically open, renewable, redactive, revenue-generating, reliable.

[0331] Leverage: In foreign currency trading, leverage multiplies the real funds in your account by a given factor, enabling you to make trades that result in significant profit. By giving leverage to a trader, the trading exchange is effectively lending them money, in the hope that it will earn back more than it loaned in commission. Leverage is also known as a margin requirement.

[0332] Lightweight Client: Comparing to full node, lightweight node does not store the whole blockchain and thus cannot fully verify any transaction. There are two kinds of lightweight nodes: those fully trusting an external service to determine wallet balance and validity of transactions (e.g. blockchain.info) and the apps implementing Simplified Payment Verification (SPV). SPV clients do not need to trust any particular service, but are more vulnerable to 51% attack than full nodes. See Simplified Payment Verification.

[0333] Litecoin: An altcoin based on the Scrypt proof of work.

[0334] Liquidity: The ability to buy and sell an asset easily, with pricing that stays roughly similar between trades. A suitably large community of buyers and sellers is important for liquidity. The result of an illiquid market is price volatility, and the inability to easily determine the value of an asset.

[0335] Liquidity Swap: As a financial instrument on cryptocurrency exchanges, liquidity swaps are contracts where investors offer loans to others to trade with in exchange for a set return.

[0336] LLL: The Lisp-like Low-level Language, a human-writable language used for authoring simple contracts and general low-level language toolkit for trans-compiling to.

[0337] Lock Time (locktime): A 32-bit field in a transaction that means either a block height at which the transaction becomes valid, or a UNIX timestamp. Zero means transaction is valid in any block. A number less than 500000000 is interpreted as a block number (the limit will be hit after year 11000), otherwise a timestamp.

[0338] Lottery: Defined by many states as prize, chance & consideration

M

[0339] MAC Media Access Control.

[0340] Main Chain: A part of the blockchain which a node considers the most difficult (see difficulty). All nodes store all valid blocks, including orphans and recompute the total difficulty when receiving another block. If the newly arrived block or blocks do not extend existing main chain, but create another one from some previous block, it is called reorganization.

[0341] Mainnet: Main Bitcoin network and its blockchain. The term is mostly used in comparison to testnet.

[0342] mBTC: 1 thousandth of a bitcoin (0.001 BTC).

[0343] Megahashes/sec: The number of hashing attempts possible in a given second, measured in millions of hashes (thousands of Kilohashes).

[0344] Mempool: A technical term for a collection of unconfirmed transactions stored by a node until they either expire or get included in the main chain. When reorganization happens, transactions from orphaned blocks either become invalid (if already included in the main chain) or moved to a pool of unconfirmed transactions. By default, bitcoind nodes throw away unconfirmed transactions after 24 hours.

[0345] Merged Mining: This allows a miner to work on multiple blockchains simultaneously, contributing to the hash rate (and thus security) of both currencies being mined. E.g. Namecoin has implemented merged mining with Bitcoin.

[0346] Merkle Tree: Merkle tree is an abstract data structure that organizes a list of data items in a tree of their hashes (like in Git, Mercurial or ZFS). In Bitcoin the merkle tree issued only to organize transactions within a block (the block header contains only one hash of a tree) so that full nodes may prune fully spent transactions to save disk space. SPV clients store only block headers and validate transactions if they are provided with a list of all intermediate hashes.

[0347] Message: Data (as a set of bytes) and Value (specified as Ether) that is passed between two Accounts, either through the deterministic operation of an Autonomous Object or the cryptographically secure signature of the Transaction.

[0348] Message Call: The act of passing a message from one Account to another. If the destination account is associated with non-empty EVM Code, then the VM will be started with the state of said Object and the Message acted upon. If the message sender is an Autonomous Object, then the Call passes any data returned from the VM operation.

[0349] Microtransaction: Paying a tiny amount for an asset or service, primarily online. Micro-transactions are difficult to perform under conventional payment systems, because of the heavy commissions involved. It is difficult to pay two cents to read an online article using your credit card, for example.

[0350] Miner: A computer participating in any cryptocurrency network performing proof of work. This is usually done to receive block awards.

[0351] Mining: The act of generating new bitcoins by solving cryptographic problems using computing hardware.

[0352] Mining Algorithm: The algorithm used by a cryptocurrency to sign transactions in the Bitcoin network, adding blocks onto the blockchain.

[0353] Mining Contract: A method of investing in bitcoin mining hardware, allowing anyone to rent out a pre-specified amount of hashing power, for an agreed amount of time. The mining service takes care of hardware maintenance, hosting and electricity costs, making it simpler for investors.

[0354] Mining Pool: A group of miners who have decided to combine their computing power for mining. This allows rewards to be distributed more consistently between participants in the pool.

[0355] Mint: Satoshi distributed the mint by linking the issuance of bitcoins to the creation of a new block ledger, putting the power to mint into all the hands of the peer network.

[0356] Mintage Cap: As cryptocurrency miners process blocks of transaction data, they generate new coins as a result. Cryptocurrency is a young industry, and its issuers want enough coins to go around to satisfy new investors as they join. These new coins are mathematically designed to be turned out at a stable rate, so the value of the currency will remain relatively stable, too (there will be fluctuations, as in any other commodity market, but not as wild as they would be if the commodity was extremely limited in availability). Over time, however, the mathematics of coin creation are also designed to end, to avoid over-saturation of the market and currency devaluation.

[0357] Minting: the process of rewarding users in proof of stake coins. New coins are minted as the reward for verifying transactions in a block.

[0358] Mixing: A process of exchanging coins with other persons in order to increase privacy of one's history. Sometimes it is associated with money laundering, but strictly speaking it is orthogonal to laundering. In traditional banking, a bank protects customer's privacy by hiding transactions from all 3rd parties. In Bitcoin any merchant may do a statistical analysis of one's entire payment history and determine, for instance, how many bitcoins one owns. While it is still possible to implement KYC (Know Your Customer) rules on a level of every merchant, mixing allows to be separate information about one's history between the merchants. Most important use cases for mixing are: 1) receiving a salary as a single bit monthly payment and then spending it in small transactions ("café sees thousands of dollars when you pay just $4"); 2) making a single payment and revealing connection of many small private spendings ("car dealer sees how much you are addicted to the coffee"). In both cases your employer, a café and a car dealer may comply with KYC/AML laws and report your identity and transferred amounts, but neither of them need to know about each other. Mixing bitcoins after receiving a salary and mixing them before making a big payment solves this privacy problem.

[0359] Mixing Service: Service that mixes your bitcoins with someone else's, sending you back bitcoins with different inputs and outputs from the ones that you sent to it. A mixing service (also known as a tumbler) preserves your privacy because it stops people tracing a particular bitcoin to you. It also has the potential to be used for money laundering.

[0360] Mobile Wallet: A wallet which runs a "Mobile client", allowing people to have bitcoin wallets on their phones and tablet computers and pay on the go.

[0361] Monetary Policy: Another breakthrough is to preserve value programmed into the software.

[0362] Money Laundering: The act of trying to "clean" money earned from criminal activity by converting these profits to what appear to be legitimate assets.

[0363] M-of-N Multi-signature Transaction: A transaction that can be spent using M signatures when N public keys are required (M is less or equal to N). Multi-signature transactions that only contain one OP_CHECKMULTSIG opcode and N is 3, 2 or 1 are considered standard.

[0364] Multisig: Multi-signature addresses allow multiple parties to partially seed an address with a public key. When someone wants to spend some of the bitcoins, they need some of these people to sign their transaction in addition to themselves. The needed number of signatures is agreed at the start when people create the address. Services using multi-signature addresses have a much greater resistance to theft.

N

[0365] Namecoin: An altcoin designed to provide an alternative to the traditional domain name system (DNS). Users can register .bit domains, accessible via proxy servers, by paying with namecoins.

[0366] Network Effect: The increase in value of a good or service that occurs when its use becomes more widespread.

[0367] NFC: Acronym for "Near Field Communication", a low power, short range method of wireless communication. This can be used to build upon RFID systems and is what contactless smart cards (oyster cards) and payment systems (paypass) use. Most recently implement in the Apple Pay app.

[0368] Node: A computer connected to the bitcoin network using a client that relays transactions to others (see client).

[0369] Nonce: A random string of data used as an input when hashing a transaction block. A nonce is used to try and produce a digest that fits the numerical parameters set by the bitcoin difficulty. A different nonce will be used with each hashing attempt, meaning that billions of nonces are generated when attempting to hash each transaction block.

[0370] Non-standard Transaction: Any valid transaction that is not standard. Non-standard transactions are not relayed or mined by default BitcoinQT nodes (but are relayed and mined on testnet). However, if anyone puts such transaction in a block, it will be accepted by all nodes. In practice it means that unusual transactions will take more time to get included in the blockchain. If some kind of non-standard transactions becomes useful and popular, it may get named standard and adopted by users (like it). See Standard Transaction.

[0371] Novacoin: Though this type of cryptocurrency is not yet near the value or overall investor numbers of the big players in the industry, Novacoin still holds a spot in the top five; not bad, considering it was introduced in February 2013. Novacoin uses the Scrypt mining algorithm, and is mined by the combined proof-of-work and proof-of-stake methods.

O

[0372] Object: Synonym for Autonomous Object.

[0373] Off Blockchain Transactions: Exchanges of value which occur off the blockchain between trusted parties. These occur because they are quicker and do not block the blockchain.

[0374] Off-Ledger Currency: A currency minted off-ledger and used on-ledger. An example of this would be using distributed ledgers to manage a national currency.

[0375] On-Ledger Currency: A currency minted on-ledger and used on-ledger. An example of this would be cryptocurrency.

[0376] Opcode: 8-bit code of script operation. Codes from 0x01 to 0x4B (decimal 75) are interpreted as a length of data to be pushed on the stack of the interpreter (data bytes follow the opcode). Other codes are either do something interesting, or disabled and cause transaction verification to fail, or do nothing (reserved for future use).

[0377] Open Network Enterprises: As smart contracts grow in complexity and interoperate with other contracts then contribute to this.

[0378] Open Source: The practice of sharing the source code for a piece of computer software, allowing it to be distributed and altered by anyone.

[0379] Orphan Block: A block which is not a part of the valid blockchain, but which was instead part of a fork that was discarded.

[0380] OTC Exchange: An exchange in which traders make deals with each other directly, rather than relying on a central exchange to mediate between them.

[0381] Output: The destination address for a bitcoin transaction. There can be multiple outputs for a single transaction.

[0382] Owners of Coin: Ethereum chose this as its economic set. Ripple and Stellar chose the social network.

[0383] Owners of the Computing Power: Satoshi chose this economic set. This requires these miners to consume a resource external to the network, namely electricity, if they want to participate in the reward system.

P

[0384] Paper Wallet: A printed sheet containing one or more public bitcoin addresses and their corresponding private keys. Often used to store bitcoins securely, instead of using software wallets, which can be corrupted, or web wallets, which can be hacked or simply disappear. A useful form of cold bitcoin storage.

[0385] Participant: An actor who can access the ledger: read records or add records to.

[0386] Pay-to-Script Hash: A type of script and address that allows sending bitcoins to arbitrary complex scripts using a compact hash of that script. This allows payer to pay much smaller transaction fees and not wait very long for a non-standard transaction to get included in the blockchain. Then the actual script matching the hash must be provided by the payee when redeeming the funds. P2SH addresses are encoded in Base58 Check just like regular public keys and start with number "3".

[0387] Peer: An actor that shares responsibility for maintaining the identity and integrity of the ledger.

[0388] P2P: Peer-to-peer. Decentralized interactions that happen between at least two parties in a highly interconnected network. An alternative system to a 'hub-and-spoke' arrangement, in which all participants in a transaction deal with each other through a single mediation point.

[0389] Permissioned Ledger: A permissioned ledger is a ledger where actors must have permission to access the ledger. Permissioned ledgers may have one or many owners. When a new record is added, the ledger's integrity is checked by a limited consensus process. This is carried out by trusted actors—government departments or banks, for example—which makes maintaining a shared record much simpler that the consensus process used by unpermissioned ledgers. Permissioned block chains provide high-verifiable data sets because the consensus process creates a digital signature, which can be seen by all parties. A permissioned ledger is usually faster than an unpermissioned ledger.

[0390] Phone-to-Phone Transfer: This is a mobile application feature that allows the instantaneous transfer of information from one smartphone to another. If two mobile device users want to exchange data, and both have this feature installed and activated on their phones, they can make the transfer simply by having their devices in close proximity to each other. These are also sometimes called "touch transfers."

[0391] Platform Exchange: This is a digital currency exchange that limits the role they play in transactions made between investors. The majority of exchanges are there to facilitate these transactions, and make them easier to carry out. The exchange will sort through buy and sell orders, and will then match up investors who meet the criteria of the order in question. Their algorithms are designed so the trades being made are both secure and fair to both parties involved. Beyond that, however, the exchange does not play any "middleman" or mediating role. This is in contrast to exchanges that will hold the transaction funds in escrow, or will discuss the details of the trade with both investors before moving forward.

[0392] Pool: A collection of mining clients which collectively mine a block, and then split the reward between them. Mining pools are a useful way to increase your probability of successfully mining a block as the difficulty rises.

[0393] PPCoin: AKA Peercoin or P2P coin. An altcoin using the proof of stake mechanism in conjunction with proof of work. Based on a paper produced by Sunny King and Scott Nadal.

[0394] Pre-mining: The mining of coins by a cryptocurrency's founder before that coin has been announced and details released to others who may wish to mine the coin. Pre-mining is a common technique used with scamcoins, although not all pre-mined coins are scamcoins (see Scamcoin).

[0395] Primecoin: Developed by Sunny King, Primecoin uses a proof of work system to calculate prime numbers.

[0396] Private Key (PrivKey): An alphanumeric string kept secret by the user, and designed to sign a digital communication when hashed with a public key. In the case of bitcoin, this string is a private key designed to work with a public key. The public key is a bitcoin address (see Bitcoin Address).

[0397] Process Node: The size of a transistor in nanometers, produced during a chip fabrication process. Smaller process nodes are more efficient.

[0398] Proof of Activity: Combines proof of work and proof of stake.

[0399] Proof of Burn: This is a method of "burning" one Proof of Work cryptocurrency in order to receive a different cryptocurrency. This is a form of "bootstrapping" one cryptocurrency off another, and is done by sending coins to a verifiable unspendable address.

[0400] Proof of Capacity: Requires miners to allot a sizeable volume of their hard drive to mining.

[0401] Proof of Existence: A service provided through the blockchain that allows anyone to anonymously and securely store a proof of existence for any document they choose online. This allows people to prove that a document existed at a certain point in time and demonstrate their ownership of it, without fear of that proof being taken from them.

[0402] Proof of Stake: An alternative to proof of work, in which your existing stake in a currency (the amount of that currency that you hold) is used to calculate the amount of that currency that you can mine.

[0403] Proof of Storage: Requires miners to allocate and share disk space in distributed cloud.

[0404] Proof of Work: A system that ties mining capability to computational power. Blocks must be hashed, which is in itself an easy computational process, but an additional variable is added to the hashing process to make it more difficult. When a block is successfully hashed, the hashing must have taken some time and computational effort. Thus, a hashed block is considered proof of work.

[0405] Prosumers: Customers who produce.

[0406] Protocol Evolution: Blockchain is the result of the natural evolution of internet protocols. Wired explains the story of how the original 1974 TCP/IP internet network protocol and Tim Berner-Lee's Hyper Text Transfer Protocol (HTTP) evolved in the same way as blockchain is evolving for the next generation of the Internet, bundling multiple protocols together to form the foundation of future frameworks and "watching the birth of the internet all over again".

[0407] PSP: Payment Service Provider. The PSP offers payment processing services for merchants who wish to accept payments online.

[0408] P2SH: See Pay-to-Script Hash.

[0409] Public Key (Pubkey): An alphanumeric string which is publicly known, and which is hashed with another, privately held string to sign a digital communication. In the case of bitcoin, the public key is a bitcoin address.

Q

[0410] QR Code: A two-dimensional graphical block containing a monochromatic pattern representing a sequence of data. QR or "Quick Response" codes are designed to be scanned by cameras, including those found in mobile phones, and are frequently used to encode bitcoin addresses.

R

[0411] Reference Implementation: Bitcoin QT (or bitcoind) is the most used full node implementation, so it is considered a reference for other implementations. If an alternative implementation is not compatible with BitcoinQT it may be forked, that is it will not see the same main chain as the rest of the network running BitcoinQT.

[0412] Relaying Transactions: Connected Bitcoin nodes relay new transactions between each other on best effort basis in order to send them to the mining nodes. Some transactions may not be relayed by all nodes. E.g. non-standard transactions, or transactions without a minimum fee. Bitcoin message protocol is not the only way to send the transaction. One may also send it directly to a miner, mine it yourself, or send it directly to the payee and make them to relay or mine it.

[0413] Remittance: A sum of money being sent, usually internationally, as a payment or gift.

[0414] Reorg, Reorganization: An event in the node when one or more blocks in the main chain become orphaned. Usually, newly received blocks are extending existing main chain. Sometimes (4-6 times a week) a couple of blocks of the same height are produced almost simultaneously and for a short period of time some nodes may see one block as a tip of the main chain which will be eventually replaced by a more difficult blocks(s). Each transaction in the orphaned blocks either becomes invalid (if already included in the main chain block) or becomes unconfirmed and moved to the mempool. In case of a major bug or a 51% attack, reorganization may involve reorganizing more than one block.

[0415] Replicated Ledger: A ledger with one master (authoritative) copy of the data, and many slave (non-authoritative) copies.

[0416] Reward: Amount of newly generated bitcoins that a miner may claim in a new block. The first transaction in the block allows miner to claim currently allowed reward as well as transaction fees from all transactions fees from all transactions in the block. Reward is halved ever 210000 blocks approximately every 4 years. As of Jul. 27, 2014 the reward is 25 BTC (the first halving occurred in December 2012). For security reasons, rewards cannot be spent before 100 blocks built on top of the current book.

[0417] Ripple: A payment network that can be used to transfer any currency (including ad hoc currencies that have been created by users). The network consists of payment nodes and gateways operated by authorities. Payments are made using a series of IOUs, and the network is based on trust relationships.

S

[0418] Satoshi: The smallest subdivision of a bitcoin currently available (0.00000001 BTC).

[0419] Satoshi Nakamoto: The name used by the original inventor of the Bitcoin protocol, who withdrew from the project at the end of 2010.

[0420] Scamcoin: An altcoin produced with the sole purpose of making money for the originator. Scamcoins frequently use pump and dump techniques and pre-mining together.

[0421] Script: A compact turing-incomplete programming language used in transaction inputs and outputs. Scripts are interpreted by a Forth-like stack machine: each operation manipulates data on the stack. Most scripts follow the standard pattern and verify the digital signature provided in the transaction input against a public key provided in the previous transaction's output. Both signatures and public keys are provided using scripts. Scripts may contain complex conditions, but can never change amounts being transferred. Amount is stored in a separate field in a transaction output.

[0422] scriptPubKey: Original name in bitcoind for a transaction output script. Typically, output scripts contain public keys (or their hashes: see Address) that allow only owner of a corresponding private key to redeem the bitcoins in the output.

[0423] scriptSig: Original name in bitcond for a transaction input script. Typically, input scripts contain signatures to prove ownership of bitcoins sent by a previous transaction.

[0424] Scrypt: An alternative proof of work system to SHA-256, designed to be particularly friendly to CPU and GPU miners, while offering little advantage to ASIC miners.

[0425] Secret Key: Either the Private Key or an encryption key is used in encrypted wallets. Bitcoin protocol does not use encryption anywhere, so secret key typically means a private key used for signing transactions.

[0426] Sequence: A 32-bit unsigned integer in a transaction input used to replace older version of a transaction by a newer one. Only used when locktime is not zero. Transaction is not considered valid until the sequence number is 0xFFFFFFFF.

[0427] Seed: The private key used in a "deterministic wallet".

[0428] Self-Executing Contract: Also known as "smart contracts" these are protocols that facilitate or enforce the obligations of contract without the need for human intervention.

[0429] SEPA: The Single European Payments Area. A payment integration agreement within the European Union, designed to make it easier to transfer funds between different banks and nations in euros.

[0430] SHA-256: The cryptographic function used as the basis for bitcoin's proof of work system.

[0431] Sidechain: These are theoretical, independent blockchains which are "two way pegged" to the Bitcoin blockchain. These can have their own unique features and can have bitcoins sent to and from them.

[0432] Signature: A digital digest produced by hashing private and public keys together to prove that a bitcoin transaction came from a particular address.

[0433] Simplified Payment Verification (SPV): A scheme to validate transactions without storing the whole blockchain (only block headers) and without trusting any external service. Every transaction must be present with all its parent and sibling hashes in a merkle tree up to the root. SPV client trusts the most difficult chain of block headers and can validate if the transaction indeed belongs to a certain block header. Since SPV does not validate all transactions, a 51% attack may not only cause a double spend (like with full nodes), but also make a completely invalid payment with bitcoins created from nowhere. However, this kind of attack is very costly and probably more expensive than a product in question. Bitcoinj library implements SPV functionally. (See SPV)

[0434] Smart Contracts: Smart contracts are contracts whose terms are recorded in a computer language instead of a legal language. Smart contracts can be automatically executed by a computing system, such as a suitable distributed ledger system.

[0435] Soft Fork: Sometimes the soft fork refers to an important change of software behavior that is not a hard fork (e.g. changing mining fee policy). See Hard Fork and Fork.

[0436] Source Code: The open-source software which includes protocols governing rules for movement and ownership of bitcoins and the cryptography system that secures and verifies Bitcoin transactions.

[0437] Speculator: An individual who speculates on the price of bitcoin or any other form of asset. Aiming to make profits by buying and selling at different prices.

[0438] Spent Output: A transaction output can be spent only once: when another valid transaction makes a reference to this output from its own input. When another transaction attempts to spend the same output, it will be rejected by the nodes already seeing the first transaction. Blockchain as a proof-of-work scheme allows every node to agree on which transaction was indeed the first one. The whole transaction is considered spent when all its outputs are spent.

[0439] Spilt: A split of a blockchain. See Fork.

[0440] SPV: Simplified Payment Verification. A feature of the Bitcoin protocol that enables nodes to verify payments without downloading the full blockchain. Instead, they need only download block headers.

[0441] Stale: When a bitcoin block is successfully hashed, any others attempting to hash it may as well stop, because it is now 'stale'. They would simply be repeating work that someone else has already done, for no reward. The term is also used in mining pools to describe a share of a hashing job that has already been completed.

[0442] Stale Block: A block that has already been solved and thus cannot offer miners any reward for further work on it.

[0443] Standard Transaction: Some transactions are considered standard, meaning they are relayed and mined by most nodes. More complex transactions could be buggy or cause DoS attacks on the network, so they are considered non-standard and not relayed or mined by most nodes. Both standard and non-standard transactions are valid and once included in the blockchain, will be recognized by all nodes. Standard transactions are: 1) sending to a public key, 2) sending to an address, 3) sending to a P2SH address, 4) sending to a M-of-N multi-signature transaction where N is 3 or less.

[0444] Storage State: The information particular to a given Account that is maintained between the times that the Account's associated EVM Code runs.

T

[0445] Taint: An analysis of how closely related two addresses are when they have both held a particular bitcoin. A taint analysis could be used to determine how many steps it took for bitcoins to move from an address known for stolen coins, to the current address.

[0446] Target: A 2.56-bit number that puts an upper limit for a block header hash to be valid. The lower the target is, the higher the difficult to find a valid has. The maximum (easiest) target is 0x00000000FFFF000000000000000000000000000000000000000000000000. The difficulty and the target are adjusted every 2016 blocks (approx. 2 weeks) to keep interval between the blocks close to 10 minutes.

[0447] TCP/IP: Acronyms stand for "Transmission Control Protocol"/"Internet Protocol" and is the connection protocol used by the Internet.

[0448] Terabashes/sec: The number of hashing attempts possible in a given second, measured in trillions of hashes (thousands of Gigahashes).

[0449] Testnet: An alternative bitcoin blockchain, used purely for testing purposes.

[0450] Testnet3: The latest version of testnet with another genesis block.

[0451] Timestamp: A proof that a piece of data existed at a certain point in time. For Bitcoin this is the cryptographic proof of when transactions have taken place.

[0452] Tokenless Ledger: A tokenless ledger refers to a distributed ledger that doesn't require a native currency to operate.

[0453] TOR: An anonymous routing protocol, used by people wanting to hide their identity online.

[0454] Total Coin Supply: For many cryptocurrencies, there is a limit on the total number of coins that will ever come into existence, bitcoin's total supply is capped at 21 million coins.

[0455] Transaction: A piece of data, signed by an External Actor. It represents either a Message or a new Autonomous Object. Transactions are recorded into each block of the blockchain.

[0456] Transaction Block: A collection of transactions on the bitcoin network, gathered into a block that can then be hashed and added to the blockchain.

[0457] Transaction Database: From a purely technological perspective, blockchains are transaction databases. The hashes, keys and nodes all make up a distributed database that eschews centralized storage

[0458] Transaction Fee: A small fee imposed on some transactions sent across the bitcoin network. The transaction fee is awarded to the miner that successfully hashes the block containing the relevant transaction.

[0459] Transaction Input: A part of a transaction that contains a reference to a previous transaction's output and a script that can prove ownership of that output. The script usually contains a signature and thus called scriptSig. Inputs spend previous outputs completely. So if one needs to pay only a portion of some previous output, the transaction should include extra change output that sends the remaining portion back to its owner (on the same or different address). Coinbase transactions contain only one input with a zeroed reference to a previous transaction and an arbitrary data in place of script.

[0460] Transaction Output: An output contains an amount to be sent and a script that allows further spending. The script typically contains a public key (or an address, a hash of a public key) and a signature verification opcode. Only an owner of a corresponding private key is able to create another transaction that sends that amount further to someone else. In every transaction, the sum of output amounts must be equal or less than a sum of all input amounts. See Change.

[0461] TX: see Transaction.

[0462] Txin: see Transaction Input.

[0463] Txout: see Transaction Output.

U

[0464] Ubiquity: Blockchains are everywhere; at this point in the alphabet that is not news. The open-source code, universally applicable architecture of blockchains, and their ability to distribute, anonymize, protect, and keep a perfectly accurate record of web transactions makes the technology a given.

[0465] Ubtc: One microbitcoin (0.000001 BTC).

[0466] Unconfirmed Transaction: Transaction that is not included in any block. Also known as "0-confirmation" transaction. Unconfirmed transactions are relayed by the nodes and stay in the mempools. Unconfirmed transaction stays in the pool until the node decides to throw it away, finds it in the blockchain, or includes it in the blockchain, or includes it in the blockchain itself (if it is a miner). See Confirmation Number.

[0467] Unique Node List: Other blockchains such as Ripple and Stellar rely on social networks for consensus and may recommend new participants (i.e., new nodes) to generate unique mode list.

[0468] Unpermissioned Ledgers: Unpermissioned ledgers such as Bitcoin have no single owner—indeed, they cannot be owned. The purpose of an unpermissioned ledger is to allow anyone to contribute data to the ledger and for everyone in possession of the ledger to have identical copies. This creates resistance which means that no actor can prevent a transaction from being added to the ledger. Participants maintain the integrity of the ledger by reaching a consensus about its state.

[0469] UTXO Set: A collection of Unspent Transaction Outputs. Typically used in discussions on optimizing an ever-growing index of transaction outputs that are not yet spent. The index is important to efficiently validate newly created transactions. Even if the rate of the new transactions remains constant, the time required to locate and verify unspent output grows. Possible technical solutions include more efficient indexing algorithms and a more performant hardware. BitcoinQT, for example, keeps only an index of outputs matching user's keys and scans the entire blockchain when validating other transactions. A developer of one web wallet service mentioned that they maintain the entire index of UTXO and its size was around 100 Gb when the blockchain itself was only Gb. Some people seek social methods to solve the problem. For instance, by refusing to relay or mine transactions that are considered dust (containing outputs smaller than a transaction fee required to mine/relay them).

V

[0470] Vanity Address: A bitcoin address with a desirable pattern, such as a name.

[0471] Varint: This term may cause confusion as it means different formats in different Bitcoin implementations. See CompactSize.

[0472] Velocity of Money: The velocity of money is an indicator of how quickly money received is then spent again. For bitcoin, we use "bitcoin days destroyed" to measure its velocity, this can indicate whether people are hoarding or spending their bitcoins.

[0473] Verification: Blockchains would not work as ledgers without verification. Much of this falls on miners, whose block creation software verifies hashes of transactions when bundling them into blocks. In cryptocurrency and banking scenarios, payment verification is also paramount. This verification happens through node communication in the distributed network, cross-checking a Bitcoin transaction against each node's blockchain data before sending it through.

[0474] Virgin Bitcoin: Bitcoins purchased as a reward for mining a block. These have not yet been spent anywhere.

[0475] Volatility: The measurement of price movements over time for a traded financial asset (including bitcoin).

W

[0476] Wallet: A method of storing bitcoins for later use. A wallet holds the private keys associated with bitcoin addresses. The blockchain is the record of the bitcoin amounts associated with those addresses.

[0477] Wallet: Just like a bill-and-coin wallet, this is a place to keep your digital currency. There are four types of cryptocurrency wallets:

[0478] 1. Software Wallet. These are programs you load onto your desktop or laptop computer.

[0479] 2. Mobile Wallet: These come in the form of applications you install on your smartphone or tablet computer. They usually include QR code scanning and phone-to-phone transfers for on-the-go transactions.

[0480] 3. Web Wallet: These are usually gotten through exchanges, and stored on third-party servers via cloud computing. They can be accessed by any computing device.

[0481] 4. Paper Wallet: Your digital currency can be printed out, usually in the form of QR codes, and these hard-copy cryptocurrency "bills" can be kept in a physical wallet just like traditional money.

[0482] Wire Transfer: Electronically transferring money from one person to another. Commonly used to send and retrieve fiat currency from bitcoin exchanges.

X

[0483] XBT: Informal currency code for 1 Bitcoin (defined as 100 000 000 Satoshis). Some people proposed using it for 0.01 Bitcoin to avoid confusion with BTC. There were rumors that Bloomberg tests XBT as a ticker for 1 Bitcoin, but currently there is only ticker XBTFUND for SecondMarket's Bitcoin Investment Trust. See BTC.

[0484] XRP: Also known as Ripple, XRP is a global payments network built on blockchain that is marketed at international banks. XRP itself is the native currency organizations can use to represent flat currency, cryptocurrency, commodities, or any other unit of value. Ripple is one of the oldest examples of open payment protocols using blockchain, but there is a laundry list of companies with different APIs, platforms and distributed payments networks. Deloitte's Banking Industry Outlook recently released a report estimating that blockchain-based payment systems could equal the volume of the United States' Automated Clearing House (ACH) financial transactions network by 2020.

Z

[0485] Zerocoin: A protocol designed to make cryptocurrency transactions truly anonymous.

[0486] Zero-confirmation Transaction: A transaction in which the merchant is happy to provide a product or service before the bitcoin's transmission has been confirmed by a miner and added to the blockchain. It can carry a risk of double spending.

[0487] Zero-confirmation Transaction: The processing of data for cryptocurrency transactions can take anywhere from half a minute upward to over ten minutes in some cases. Though this is necessary in order to validate transactions, and guards against fraudulent activity such as double spending, the waiting period can be inconvenient for those involved in the transactions. As a result, some exchanges and businesses that deal with digital currency are offering "zero confirmation" transactions, which are almost immediately verified without waiting for the mining process to confirm the data block. Double spending, the practice in which a coin holder applies the same currency to two different transactions is a concern with zero confirmation transactions. Since cryptocurrency is not "attached" to the person spending it in any way, by the time their double spending is discovered through the mining process, they are long gone and untraceable. With the demand for zero confirmation transactions on the upswing, entrepreneurs in the cryptocurrency industry are looking at ways to instantly verify, or deny, transactions without having to wait for mining to take place. In the meantime, many businesses levy fees to offset the financial risk of zero confirmation transactions, and yet others are refusing to accept them until the technology catches up.

[0488] Z System: IBM is openly committed to advancing blockchain technology on many fronts, but the company has even gone as far as offering a Blockchain-as-a-Service (BaaS) platform for developers on the IBM Cloud, and integrating blockchain-based apps (created through the Hyperledger Project) on IBM z Systems. IBM even plans to leverage blockchains combined with Watson on the Watson IoT platform to make it possible for information from devices such as RFID-based locations, barcode-scan event, or device-reported data to be used with IBM's Blockchain and sync with distributed ledgers and smart contracts.

We claim:

1. A system for control of a transaction state system utilizing a distributed ledger, comprising:

an application plane layer, the application layer adapted to receive instructions regarding operation of the transaction state system, the application plane layer coupled to an application plane layer interface,

a control plane layer, the control plane layer including an adaptive control unit, the control plane layer interfacing with the application plane layer via the application plane layer interface to receive information related to the instructions regarding operation of the transaction state system, and

a data plane layer, the data plane layer including an input interface to receive data input from one or more data sources and to provide output coupled to a decentralized distributed ledger, the data plane layer being coupled to the control plane layer.

2. The system for the control of a transaction state system of claim **1** wherein decentralized distributed ledger stores data on cryptocurrency.

3. The system for the control of a transaction state system of claim **1** wherein the adaptive control unit includes cognitive computing unit.

4. The system for control of a transaction state system of claim **1** wherein the control plane layer includes an artificial intelligence unit.

5. The system for control of a transaction state system of claim **1** wherein the control plane layer includes a machine-learning unit.

6. The system for control of a transaction state system of claim **1** wherein the control plane layer includes a neural network.

7. The system for control of a transaction state system of claim **6** wherein the neural network is a deep neural network.

8. The system for control of a transaction state system of claim **6** wherein the neural network includes a graphics processing unit (GPU).

9. The system for control of a transaction state system of claim **6** wherein the neural network is trained utilizing user response data.

10. The system for control of a transaction state system of claim **6** wherein the neural network is a vectorized neural network.

11. The system for control of a transaction state system of claim **6** wherein the neural network is a recurrent neural network.

12. The system for control of a transaction state system of claim **1** wherein the control plan layer includes an analytics unit.

13. The system for control of a transaction state system of claim **1**, wherein the control plane layer further includes a processor.

14. The system for control of a transaction state system of claim **1** wherein the application plane layer includes a graphical user interface unit.

15. The system for control of a transaction state system of claim **1** wherein the application play layer further includes a processor.

16. The system for control of a transaction state system of claim **1** wherein the data plane layer includes an input port.

17. The system for control of a transaction state system of claim **1** wherein the input port is coupled to receive external data.

18. The system for control of a transaction state system of claim **17** wherein the external data in Internet of Things (IoT) data.

19. The system for control of a transaction stale system of claim **17** wherein the input port is coupled to a processor.

20. The system for control of a transaction state system of claim **1** wherein the data plane layer includes a graphical user interface (GUI) generator.

21. The system for control of a transaction state system of claim **20** wherein the graphical user interface is coupled to an output port.

22. The system for control of a transaction state system of claim **21** wherein the data plane layer includes an output port adapted to couple to a display device.

23. The system for control of a transaction state system of claim **1** wherein the data plane layer further includes a value transfer element.

24. The system for control of a transaction state system of claim **1** wherein the data plane layer further includes a title transfer element.

25. The system for control of a transaction state system of claim **1** wherein the data plane layer further includes a management network element.

26. The system for control of a transaction state system of claim **1** wherein the data plane layer further includes a control network element.

* * * * *